Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
adaltas					
mixme					
N/A	03-05-2021	6.4	In Node.js mixme, prior to v0.5.1, an attacker can add or alter properties of an object via '__proto__' through the mutate() and merge() functions. The polluted attribute will be directly assigned to every object in the program. This will put the availability of the program at risk causing a potential denial of service (DoS). **CVE ID : CVE-2021-28860**	https://github.com/adaltas/node-mixme/commit/cfd5fbfc32368bcf7e06d1c5985ea60e34cd4028	A-ADA-MIXM-010621/1
algorithmica_project					
algorithmica					
Double Free	03-05-2021	5	An issue was discovered in the algorithmica crate through 2021-03-07 for Rust. There is a double free in merge_sort::merge(). **CVE ID : CVE-2021-31996**	https://rustsec.org/advisories/RUSTSEC-2021-0053.html	A-ALG-ALGO-010621/2
aomedia					
aomedia					
Release of Invalid Pointer or Reference	06-05-2021	7.5	aom_image.c in libaom in AOMedia before 2021-04-07 frees memory that is not located on the heap. **CVE ID : CVE-2021-30473**	https://aomedia.googlesource.com/aom/+/4efe20e99dcd9b6f8eadc8de8acc825be7416578	A-AOM-AOME-010621/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apache					
airflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-05-2021	4.3	The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions <1.10.15 in 1.x series and affects 2.0.0 and 2.0.1 and 2.x series. This is the same as CVE-2020-13944 & CVE-2020-17515 but the implemented fix did not fix the issue completely. Update to Airflow 1.10.15 or 2.0.2. Please also update your Python version to the latest available PATCH releases of the installed MINOR versions, example update to Python 3.6.13 if you are on Python 3.6. (Those contain the fix for CVE-2021-23336 https://nvd.nist.gov/vuln/detail/CVE-2021-23336). **CVE ID : CVE-2021-28359**	https://lists.apache.org/thread.html/ra8ce70088ba291f358e077cafdb14d174b7a1ce9a9d86d1b332d6367%40%3Cusers.airflow.apache.org%3E, https://lists.apache.org/thread.html/rc005f4de9d9b0ba943ceb8ff5a21a5c6ff8a9df52632476698d99432@%3Cannounce.apache.org%3E	A-APA-AIRF-010621/4
unomi					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	04-05-2021	5	Apache Unomi prior to version 1.5.5 allows CRLF log injection because of the lack of escaping in the log statements. **CVE ID : CVE-2021-31164**	http://unomi.apache.org/security/cve-2021-31164	A-APA-UNOM-010621/5
apollo13themes					
rife_elementor_extensions_\\&_templates					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Rife Elementor Extensions & Templates" WordPress Plugin before 1.1.6 has a widget that is vulnerable to stored Cross-Site Scripting(XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24265**	https://wpscan.com/vulnerability/9f4771dc-80b5-49ff-9f64-bf6c36f76863	A-APO-RIFE-010621/6
arcgis					
geoevent_server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-05-2021	5	ArcGIS GeoEvent Server versions 10.8.1 and below has a read-only directory path traversal vulnerability that could allow an unauthenticated, remote attacker to perform directory traversal attacks and read arbitrary files on the system. **CVE ID : CVE-2021-29101**	https://www.esri.com/arcgis-blog/products/ext-server-geoevent/administration/arcgis-geoevent-server-security-update-2021-patch-1	A-ARC-GEOE-010621/7
Artica					
pandora_fms					
Deserialization of Untrusted Data	07-05-2021	7.5	Artica Pandora FMS 742 allows unauthenticated attackers to perform Phar deserialization. **CVE ID : CVE-2021-32098**	https://pandorafms.com/blog/whats-new-in-pandora-fms-743/	A-ART-PAND-010621/8
Improper Neutralization of Special Elements used in an SQL	07-05-2021	7.5	A SQL injection vulnerability in the pandora_console component of Artica Pandora FMS 742 allows an unauthenticated attacker to	https://pandorafms.com/blog/whats-new-in-pandora-fms-743/	A-ART-PAND-010621/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			upgrade his unprivileged session via the /include/chart_generator.php session_id parameter, leading to a login bypass. **CVE ID : CVE-2021-32099**		
N/A	07-05-2021	4	A remote file inclusion vulnerability exists in Artica Pandora FMS 742, exploitable by the lowest privileged user. **CVE ID : CVE-2021-32100**	https://pandorafms.com/blog/whats-new-in-pandora-fms-743/	A-ART-PAND-010621/10
blocksera					
image_hover_effects					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Image Hover Effects – Elementor Addon" WordPress Plugin before 1.3.4 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24264**	https://wpscan.com/vulnerability/7fd89a49-fbb0-4308-836b-1f12dc585b1f	A-BLO-IMAG-010621/11
brainstormforce					
elementor_-_header\\,_footer_\\&_blocks_template					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Elementor – Header, Footer & Blocks Template" WordPress Plugin before 1.5.8 has two widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24256**	https://wpscan.com/vulnerability/a9412fed-aed3-4931-a504-1a86f876892e	A-BRA-ELEM-010621/12
brinstormforce					
ultimate_addons_for_elementor					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Ultimate Addons for Elementor" WordPress Plugin before 1.30.0 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24271**	https://wpscan.com/vulnerability/1ce8e188-6ded-413e-b4d1-bf80258acf79	A-BRI-ULTI-010621/13
btcpayserver					
btcpay_server					
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-05-2021	5	BTCPay Server through 1.0.7.0 uses a weak method Next to produce pseudo-random values to generate a legacy API key. **CVE ID : CVE-2021-29245**	https://blog.btcpayserver.org/vulnerability-disclosure-v1-0-7-0/	A-BTC-BTCP-010621/14
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-05-2021	6.5	BTCPay Server through 1.0.7.0 suffers from directory traversal, which allows an attacker with admin privileges to achieve code execution. The attacker must craft a malicious plugin file with special characters to upload the file outside of the restricted directory. **CVE ID : CVE-2021-29246**	https://blog.btcpayserver.org/vulnerability-disclosure-v1-0-7-0/	A-BTC-BTCP-010621/15
Exposure of Sensitive Information to an Unauthorized Actor	05-05-2021	5	BTCPay Server through 1.0.7.0 could allow a remote attacker to obtain sensitive information, caused by failure to set the HTTPOnly flag for a cookie. **CVE ID : CVE-2021-29247**	https://blog.btcpayserver.org/vulnerability-disclosure-v1-0-7-0/	A-BTC-BTCP-010621/16
Exposure of Sensitive	05-05-2021	5	BTCPay Server through 1.0.7.0 could allow a	https://blog.btcpayserve	A-BTC-BTCP-010621/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information to an Unauthorized Actor			remote attacker to obtain sensitive information, caused by failure to set the Secure flag for a cookie. **CVE ID : CVE-2021-29248**	r.org/vulnerability-disclosure-v1-0-7-0/	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	BTCPay Server through 1.0.7.0 suffers from a Stored Cross Site Scripting (XSS) vulnerability within the POS Add Products functionality. This enables cookie stealing. **CVE ID : CVE-2021-29250**	https://blog.btcpayserver.org/vulnerability-disclosure-v1-0-7-0/	A-BTC-BTCP-010621/18
Centreon					
centreon_web					
Incorrect Default Permissions	04-05-2021	4	Insecure Permissions in Centreon Web versions 19.10.18, 20.04.8, and 20.10.2 allows remote attackers to bypass validation by changing any file extension to ".gif", then uploading it in the "Administration/ Parameters/ Images" section of the application. **CVE ID : CVE-2021-26804**	N/A	A-CEN-CENT-010621/19
Cisco					
anyconnect_secure_mobility_client					
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6	A-CIS-ANYC-010621/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1426**		
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1427**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6	A-CIS-ANYC-010621/21
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-ANYC-010621/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1428**	anyconnect-code-exec-jR3tWTA6	
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1429**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6	A-CIS-ANYC-010621/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1430**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6	A-CIS-ANYC-010621/24
Uncontrolled Search Path Element	06-05-2021	7.2	Multiple vulnerabilities in the install, uninstall, and upgrade processes of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. A successful exploit could allow the attacker to execute arbitrary code on an affected device with SYSTEM privileges. To exploit these vulnerabilities, the attacker must have valid credentials on the Windows system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6	A-CIS-ANYC-010621/25

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1496**		
Improper Input Validation	06-05-2021	2.1	A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software could allow an authenticated, local attacker to overwrite VPN profiles on an affected device. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to modify VPN profile files. To exploit this vulnerability, the attacker must have valid credentials on the affected system. **CVE ID : CVE-2021-1519**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-profile-AggMUCDg	A-CIS-ANYC-010621/26
broadworks_messaging_server					
Improper Restriction of XML External Entity Reference	06-05-2021	5.5	A vulnerability in the web-based management interface of Cisco BroadWorks Messaging Server Software could allow an authenticated, remote attacker to access sensitive information or cause a partial denial of service (DoS) condition on an affected system. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bwms-xxe-uSLrZgKs	A-CIS-BROA-010621/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a partial DoS condition on an affected system. There are workarounds that address this vulnerability. **CVE ID : CVE-2021-1530**		
content_security_management_appliance					
Improper Privilege Management	06-05-2021	7.2	A vulnerability in the user account management system of Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an authenticated, local attacker to elevate their privileges to root. This vulnerability is due to a procedural flaw in the password generation algorithm. An attacker could exploit this vulnerability by enabling specific Administrator-only features and connecting to the appliance through the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-priv-esc-JJ8zxQsC	A-CIS-CONT-010621/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CLI with elevated privileges. A successful exploit could allow the attacker to execute arbitrary commands as root and access the underlying operating system. To exploit this vulnerability, the attacker must have valid Administrator credentials. **CVE ID : CVE-2021-1447**		
Inclusion of Sensitive Information in Source Code	06-05-2021	4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. **CVE ID : CVE-2021-1516**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H	A-CIS-CONT-010621/29
email_security_appliance					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Sensitive Information in Source Code	06-05-2021	4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. **CVE ID : CVE-2021-1516**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H	A-CIS-EMAI-010621/30
hosted_collaboration_mediation_fulfillment					
N/A	06-05-2021	6.8	A vulnerability in the Java Management Extensions (JMX) component of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-dos-OO4SRYEf	A-CIS-HOST-010621/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an affected system. This vulnerability is due to an unsecured TCP/IP port. An attacker could exploit this vulnerability by accessing the port and restarting the JMX process. A successful exploit could allow the attacker to cause a DoS condition on an affected system. **CVE ID : CVE-2021-1478**		
integrated_management_controller					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	A-CIS-INTE-010621/32
ironport_web_security_appliance					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Sensitive Information in Source Code	06-05-2021	4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. **CVE ID : CVE-2021-1516**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H	A-CIS-IRON-010621/33
sd-wan_vbond_orchestrator					
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	A-CIS-SD-W-010621/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**		
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	A-CIS-SD-W-010621/35
sd-wan_vmanage					
Uncontrolled Resource Consumption	06-05-2021	7.8	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ	A-CIS-SD-W-010621/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1275**		
Improper Access Control	06-05-2021	5.8	A vulnerability in the web-based messaging service interface of Cisco SD-WAN vManage Software could allow an unauthenticated, adjacent attacker to bypass authentication and authorization and modify the configuration of an affected system. To exploit this vulnerability, the attacker must be able to access an associated Cisco SD-WAN vEdge device. This vulnerability is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based messaging service interface of an affected system. A successful exploit could allow the attacker to gain unauthenticated read and write access to the affected vManage system. With this access, the attacker could access information about the affected vManage system, modify the configuration of the system, or make configuration changes to devices that are managed by the system.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-auth-bypass-65aYqcS2	A-CIS-SD-W-010621/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1284		
Improper Authentication	06-05-2021	7.5	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1468**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ	A-CIS-SD-W-010621/38
Observable Discrepancy	06-05-2021	5	A vulnerability in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to enumerate user accounts. This vulnerability is due to the improper handling of HTTP headers. An attacker could exploit this vulnerability by sending authenticated requests to an affected system. A successful exploit could allow the attacker to compare the HTTP responses that are returned by the affected system to determine which accounts are valid user accounts. **CVE ID : CVE-2021-1486**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-enumeration-64eNnDKy	A-CIS-SD-W-010621/39
Improper Privilege	06-05-2021	6.5	Multiple vulnerabilities in Cisco SD-WAN vManage	https://tools.cisco.com/	A-CIS-SD-W-010621/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1505**	security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ	
Missing Authorization	06-05-2021	6.5	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1506**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ	A-CIS-SD-W-010621/41
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	3.5	A vulnerability in an API of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the application web-based interface. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-	A-CIS-SD-W-010621/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the API does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending malicious input to the API. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1507**	xss-eN75jxtW	
Missing Authorization	06-05-2021	6.5	Multiple vulnerabilities in Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information, or allow an authenticated, local attacker to gain escalated privileges or gain unauthorized access to the application. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1508**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ	A-CIS-SD-W-010621/43
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-	A-CIS-SD-W-010621/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	A-CIS-SD-W-010621/45
Improper Access Control	06-05-2021	3.3	A vulnerability in Cisco SD-WAN vManage Software could allow an unauthenticated, adjacent attacker to gain access to sensitive information. This vulnerability is due to improper access controls on API endpoints when Cisco SD-WAN vManage	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-	A-CIS-SD-W-010621/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software is running in multi-tenant mode. An attacker with access to a device that is managed in the multi-tenant environment could exploit this vulnerability by sending a request to an affected API endpoint on the vManage system. A successful exploit could allow the attacker to gain access to sensitive information that may include hashed credentials that could be used in future attacks. **CVE ID : CVE-2021-1515**	vmanage-9VZO4gfU	
Exposure of Sensitive System Information to an Unauthorized Control Sphere	06-05-2021	5	A vulnerability in the cluster management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to view sensitive information on an affected system. To be affected by this vulnerability, the Cisco SD-WAN vManage Software must be in cluster mode. This vulnerability is due to the absence of authentication for sensitive information in the cluster management interface. An attacker could exploit this vulnerability by sending a crafted request to the cluster management interface of an affected system. A successful exploit could allow the attacker to allow the attacker to view	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vmanageinfdis-LKrFpbv	A-CIS-SD-W-010621/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information on the affected system. **CVE ID : CVE-2021-1535**		
telepresence_collaboration_endpoint					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-05-2021	4	A vulnerability in the video endpoint API (xAPI) of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, remote attacker to read arbitrary files from the underlying operating system. This vulnerability is due to insufficient path validation of command arguments. An attacker could exploit this vulnerability by sending a crafted command request to the xAPI. A successful exploit could allow the attacker to read the contents of any file that is located on the device filesystem. **CVE ID : CVE-2021-1532**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-rmos-fileread-pE9sL3g	A-CIS-TELE-010621/48
ucs_manager					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	A-CIS-UCS_-010621/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
unified_communications_manager					
N/A	06-05-2021	6.8	A vulnerability in the Java Management Extensions (JMX) component of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. This vulnerability is due to an unsecured TCP/IP port. An attacker could exploit this vulnerability by accessing the port and restarting the JMX process. A successful exploit could allow the attacker to cause a DoS condition on an affected system. **CVE ID : CVE-2021-1478**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucm-dos-OO4SRYEf	A-CIS-UNIF-010621/50
unified_communications_manager_im_and_presence_service					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-05-2021	5.5	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities are due to improper validation of user-submitted parameters. An attacker could exploit these vulnerabilities by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database. **CVE ID : CVE-2021-1363**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-inj-ereCOKjR	A-CIS-UNIF-010621/51
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-05-2021	5.5	Multiple vulnerabilities in the web-based management interface of Cisco Unified Communications Manager IM & Presence Service could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. These vulnerabilities are due to improper validation of user-submitted parameters. An attacker could exploit these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-inj-ereCOKjR	A-CIS-UNIF-010621/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data or modify data that is stored in the underlying database. **CVE ID : CVE-2021-1365**		
web_security_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	4.3	A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by persuading a user to retrieve a crafted file that contains malicious payload and upload it to the affected device. 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-2021-1490**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-xss-mVjOWchB	A-CIS-WEB_-010621/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Sensitive Information in Source Code	06-05-2021	4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. **CVE ID : CVE-2021-1516**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H	A-CIS-WEB_-010621/54
classyfrieds_project					
classyfrieds					
Unrestricted Upload of File with Dangerous Type	06-05-2021	6.5	The Classyfrieds WordPress plugin through 3.8 does not properly check the uploaded file when an authenticated user adds a listing, only checking the content-type in the request. This allows any authenticated user to upload arbitrary PHP files via the Add Listing feature	https://wpscan.com/vulnerability/ee42c233-0ff6-4b27-a5ec-ad3246bef079	A-CLA-CLAS-010621/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the plugin, leading to RCE. **CVE ID : CVE-2021-24253**		
clever_addons_for_elementor_project					
clever_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Clever Addons for Elementor" WordPress Plugin before 2.1.0 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24273**	https://wpscan.com/vulnerability/70ddb3fd-d819-4d85-9f8b-1451a3e3e5a6	A-CLE-CLEV-010621/56
codeinitiator					
fitness_calculators					
Cross-Site Request Forgery (CSRF)	05-05-2021	4.3	The fitness calculators WordPress plugin before 1.9.6 add calculators for Water intake, BMI calculator, protein Intake, and Body Fat and was lacking CSRF check, allowing attackers to make logged in users perform unwanted actions, such as change the calculator headers. Due to the lack of sanitisation, this could also lead to a Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24272**	https://wpscan.com/vulnerability/e643040b-1f3b-4c13-8a20-acfd069dcc4f	A-COD-FITN-010621/57
Codesys					
automation_server					
Cross-Site Request Forgery (CSRF)	03-05-2021	6.8	CODESYS Automation Server before 1.16.0 allows cross-site request forgery (CSRF).	https://customers.codesys.com/index.php, https://ww	A-COD-AUTO-010621/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29238	w.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14638&token=30b75ee95d0d94527894dfd8cdc5432575a8eff8&download=	
conrol_runtime_system_toolkit					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONR-010621/59
control_for_beaglebone_sl					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	A-COD-CONT-010621/60
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7	A-COD-CONT-010621/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				873&download=	
control_for_empc-a\\/imx6_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	A-COD-CONT-010621/62
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0	A-COD-CONT-010621/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				f7505e29beefa5b3f8ac7873&download=	
control_for_iot2000_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	A-COD-CONT-010621/64
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&t	A-COD-CONT-010621/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				oken=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	
control_for_linux_arm_sl					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/66
control_for_linux_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/inde	A-COD-CONT-010621/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				x.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/68
control_for_pfc100_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://cust	A-COD-CONT-010621/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				omers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html , https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/70
control_for_pfc200_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html	A-COD-CONT-010621/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html , https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/72
control_for_plcnext_sl					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and	https://customers.codesys.com/index.php, https://www.codesys.com/security	A-COD-CONT-010621/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	
control_for_raspberry_pi_sl					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	A-COD-CONT-010621/74
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to	https://customers.codesys.com/index.php, https://ww	A-COD-CONT-010621/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	w.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29befa5b3f8ac7873&download=	
control_for_wago_touch_panels_600_sl					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29befa5b3f8ac7873&download=	A-COD-CONT-010621/76
control_rte					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/77
control_runtime_system_toolkit					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e	A-COD-CONT-010621/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				14799&download=	
control_win					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-CONT-010621/79
development_system					
Insufficient Verification of Data Authenticity	03-05-2021	4.6	CODESYS Development System 3 before 3.5.17.0 displays or executes malicious documents or files embedded in libraries without first checking their validity. **CVE ID : CVE-2021-29239**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14639&token=fa836f	A-COD-DEVE-010621/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				8bd4a2184aa9323a639ca9f2aaf1538412&download=	
N/A	04-05-2021	6.8	The Package Manager of CODESYS Development System 3 before 3.5.17.0 does not check the validity of packages before installation and may be used to install CODESYS packages with malicious content. **CVE ID : CVE-2021-29240**	https://customers.codesys.com/index.php, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14636&token=1ce7e6e4cbe4651989ede418450d7c82e972bdf2&download=, https://www.codesys.com/security/security-reports.html	A-COD-DEVE-010621/81
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd7	A-COD-DEVE-010621/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5ae7553ae3be25e22f741db783b31e14799&download=	
edge_gateway					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	A-COD-EDGE-010621/83
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f	A-COD-EDGE-010621/84

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	
embedded_target_visu_toolkit					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-EMBE-010621/85
gateway					
NULL Pointer Dereference	03-05-2021	5	CODESYS Gateway 3 before 3.5.17.0 has a NULL pointer dereference that may result in a denial of service (DoS). **CVE ID : CVE-2021-29241**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codes	A-COD-GATE-010621/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ys.com/index.php?eID=dumpFile&t=f&f=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&download=	
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html , https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-GATE-010621/87
hmi					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages.	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html ,	A-COD-HMI-010621/88

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-29242	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29befa5b3f8ac7873&download=	
opc_server					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29befa5b3f8ac7873&download=	A-COD-OPC_-010621/89
plchandler					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and	https://customers.codesys.com/index.php, https://www.codesys.com/security	A-COD-PLCH-010621/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	
remote_target_visu_toolkit					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-REMO-010621/91
safety_sil					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted	https://customers.codesys.com/index.php,	A-COD-SAFE-010621/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	
simulation_runtime					
Improper Input Validation	03-05-2021	7.5	CODESYS Control Runtime system before 3.5.17.0 has improper input validation. Attackers can send crafted communication packets to change the router's addressing scheme and may re-route, add, remove or change low level communication packages. **CVE ID : CVE-2021-29242**	https://customers.codesys.com/index.php, https://www.codesys.com/security/security-reports.html, https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=	A-COD-SIMU-010621/93
college_publisher_import_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
college_publisher_import					
Unrestricted Upload of File with Dangerous Type	06-05-2021	6.5	The College publisher Import WordPress plugin through 0.1 does not check for the uploaded CSV file to import, allowing high privilege users to upload arbitrary files, such as PHP, leading to RCE. Due to the lack of CSRF check, the issue could also be exploited via a CSRF attack. **CVE ID : CVE-2021-24254**	https://wpscan.com/vulnerability/bb3e56dd-ae2e-45c2-a6c9-a59ae5fc1dc4	A-COL-COLL-010621/94
coolkit					
ewelink					
Incorrect Authorization	06-05-2021	2.1	Unconstrained Web access to the device's private encryption key in the QR code pairing mode in the eWeLink mobile application (through 4.9.2 on Android and through 4.9.1 on iOS) allows a physically proximate attacker to eavesdrop on Wi-Fi credentials and other sensitive information by monitoring the Wi-Fi spectrum during a device pairing process. **CVE ID : CVE-2021-27941**	N/A	A-COO-EWEL-010621/95
Craftcms					
craft_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	4.3	Craft CMS before 3.6.13 has an XSS vulnerability. **CVE ID : CVE-2021-32470**	https://github.com/craftcms/cms/commit/f9378aa154b5f9b64bed3d59cce0c4a8184bf5e6	A-CRA-CRAF-010621/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
crocoblock					
jetwidgets_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "JetWidgets For Elementor" WordPress Plugin before 1.0.9 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24268**	https://wpscan.com/vulnerability/68ecb965-2a9d-4e67-b069-c3dbfb14016b	A-CRO-JETW-010621/97
daggerhartlab					
openid_connect_generic_client					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	4.3	The OpenID Connect Generic Client WordPress plugin 3.8.0 and 3.8.1 did not sanitise the login error when output back in the login form, leading to a reflected Cross-Site Scripting issue. This issue does not require authentication and can be exploited with the default configuration. **CVE ID : CVE-2021-24214**	https://wpscan.com/vulnerability/31cf0dfb-4025-4898-a5f4-fc7115565a10	A-DAG-OPEN-010621/98
Dell					
dbutil_2_3.sys					
Incorrect Authorization	04-05-2021	4.6	Dell dbutil_2_3.sys driver contains an insufficient access control vulnerability which may lead to escalation of privileges, denial of service, or information disclosure. Local authenticated user access is required. **CVE ID : CVE-2021-21551**	https://www.dell.com/support/kbdoc/en-us/000186019/dsa-2021-088-dell-client-platform-security-update-for-dell-driver-	A-DEL-DBUT-010621/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				insufficient-access-control-vulnerability	
dethemekit_for_elementor_project					
dethemekit_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "DeTheme Kit for Elementor" WordPress Plugin before 1.5.5.5 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24270**	https://wpscan.com/vulnerability/67967784-18b6-4e41-9597-3a4c051f3978	A-DET-DETH-010621/100
Djangoproject					
django					
Unrestricted Upload of File with Dangerous Type	05-05-2021	5	In Django 2.2 before 2.2.21, 3.1 before 3.1.9, and 3.2 before 3.2.1, MultiPartParser, UploadedFile, and FieldFile allowed directory traversal via uploaded files with suitably crafted file names. **CVE ID : CVE-2021-31542**	https://www.djangoproject.com/weblog/2021/may/04/security-releases/, https://docs.djangoproject.com/en/3.2/releases/security/, http://www.openwall.com/lists/oss-security/2021/05/04/3	A-DJA-DJAN-010621/101
emlog					
emlog					
Unrestricted Upload of File with	06-05-2021	7.5	emlog v5.3.1 and emlog v6.0.0 have a Remote Code Execution vulnerability due	N/A	A-EML-EMLO-010621/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			to upload of database backup file in admin/data.php. **CVE ID : CVE-2021-31737**		
ENG					
knowage					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-05-2021	3.5	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in '/knowage/restful-services/signup/update' via the 'surname' parameter. **CVE ID : CVE-2021-30211**	N/A	A-ENG-KNOW-010621/103
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-05-2021	3.5	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in '/knowage/restful-services/documentnotes/saveNote' via the 'nota' parameter. **CVE ID : CVE-2021-30212**	N/A	A-ENG-KNOW-010621/104
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-05-2021	4.3	Knowage Suite 7.3 is vulnerable to unauthenticated reflected cross-site scripting (XSS). An attacker can inject arbitrary web script in '/servlet/AdapterHTTP' via the 'targetService' parameter. **CVE ID : CVE-2021-30213**	N/A	A-ENG-KNOW-010621/105
Improper Neutralization of Special Elements in Output Used	12-05-2021	3.5	Knowage Suite 7.3 is vulnerable to Stored Client-Side Template Injection in '/knowage/restful-	N/A	A-ENG-KNOW-010621/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			services/signup/update' via the 'name' parameter. **CVE ID : CVE-2021-30214**		
Esri					
arcgis_earth					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-05-2021	6.8	A path traversal vulnerability exists in Esri ArcGIS Earth versions 1.11.0 and below which allows arbitrary file creation on an affected system through crafted input. An attacker could exploit this vulnerability to gain arbitrary code execution under security context of the user running ArcGIS Earth by inducing the user to upload a crafted file to an affected system. **CVE ID : CVE-2021-29100**	https://www.esri.com/arcgis-blog/products/arcgis-earth/administration/arcgis-earth-security-update	A-ESR-ARCG-010621/107
eventlet					
eventlet					
Uncontrolled Resource Consumption	07-05-2021	5	Eventlet is a concurrent networking library for Python. A websocket peer may exhaust memory on Eventlet side by sending very large websocket frames. Malicious peer may exhaust memory on Eventlet side by sending highly compressed data frame. A patch in version 0.31.0 restricts websocket frame to reasonable limits. As a workaround, restricting memory usage via OS limits would help against overall machine	https://github.com/eventlet/eventlet/security/advisories/GHSA-9p9m-jm8w-94p2	A-EVE-EVEN-010621/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhaustion, but there is no workaround to protect Eventlet process. **CVE ID : CVE-2021-21419**		
Exim					
exim					
Improper Privilege Management	06-05-2021	6.3	Exim 4 before 4.94.2 has Execution with Unnecessary Privileges. By leveraging a delete_pid_file race condition, a local user can delete arbitrary files as root. This involves the -oP and -oPX options. **CVE ID : CVE-2021-27216**	https://www.exim.org/static/doc/security/CVE-2020-qualys/CVE-2020-28007-LFDIR.txt	A-EXI-EXIM-010621/109
Foxitsoftware					
foxit_reader					
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13101. **CVE ID : CVE-2021-31441**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13239. **CVE ID : CVE-2021-31442**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/111
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object.	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13240. **CVE ID : CVE-2021-31443**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13241. **CVE ID : CVE-2021-31444**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/113
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13244. **CVE ID : CVE-2021-31445**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process. Was ZDI-CAN-13245. **CVE ID : CVE-2021-31446**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13269. **CVE ID : CVE-2021-31447**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/116
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13273. **CVE ID : CVE-2021-31448**		
Double Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13280. **CVE ID : CVE-2021-31449**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/118
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User	https://www.foxitsoftware.com/support/security-	A-FOX-FOXI-010621/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13084. **CVE ID : CVE-2021-31450**	bulletins.php	
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13089. **CVE ID : CVE-2021-31451**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13091. **CVE ID : CVE-2021-31452**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/121
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. Was ZDI-CAN-13092. **CVE ID : CVE-2021-31453**		
Heap-based Buffer Overflow	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Decimal element. A crafted leadDigits value in a Decimal element can trigger an overflow of a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current process. Was ZDI-CAN-13095. **CVE ID : CVE-2021-31454**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/123
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXI-010621/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13100. **CVE ID : CVE-2021-31455**		
phantompdf					
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13101. **CVE ID : CVE-2021-31441**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/125
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13239. **CVE ID : CVE-2021-31442**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13240. **CVE ID : CVE-2021-31443**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13241. **CVE ID : CVE-2021-31444**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/128
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13244. **CVE ID : CVE-2021-31445**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13245. **CVE ID : CVE-2021-31446**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/130
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit	https://www.foxitsoftware.com/support/security-	A-FOX-PHAN-010621/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13269. **CVE ID : CVE-2021-31447**	bulletins.php	
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13273. **CVE ID : CVE-2021-31448**		
Double Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13280. **CVE ID : CVE-2021-31449**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/133
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13084. **CVE ID : CVE-2021-31450**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13089. **CVE ID : CVE-2021-31451**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/135
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the handling of XFA forms. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13091. **CVE ID : CVE-2021-31452**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13092. **CVE ID : CVE-2021-31453**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/137
Heap-based Buffer Overflow	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to	https://www.foxitsoftware.com/support/security-	A-FOX-PHAN-010621/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Decimal element. A crafted leadDigits value in a Decimal element can trigger an overflow of a fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current process. Was ZDI-CAN-13095. **CVE ID : CVE-2021-31454**	bulletins.php	
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13100. **CVE ID : CVE-2021-31455**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13102. **CVE ID : CVE-2021-31456**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/140
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of the current process. Was ZDI-CAN-13147. **CVE ID : CVE-2021-31457**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13150. **CVE ID : CVE-2021-31458**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/142
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13162. **CVE ID : CVE-2021-31459**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13096. **CVE ID : CVE-2021-31460**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/144
Access of Resource Using Incompatible Type ('Type Confusion')	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the the handling of app.media objects. The issue results from the lack of proper	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-PHAN-010621/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-13333. **CVE ID : CVE-2021-31461**		
reader					
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13102. **CVE ID : CVE-2021-31456**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-010621/146
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-010621/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13147. **CVE ID : CVE-2021-31457**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13150. **CVE ID : CVE-2021-31458**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-010621/148
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to	https://www.foxitsoftware.com/support/security-	A-FOX-READ-010621/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13162. **CVE ID : CVE-2021-31459**	bulletins.php	
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13096. **CVE ID : CVE-2021-31460**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-READ-010621/150
Access of Resource Using	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected	https://www.foxitsoftware.com/sup	A-FOX-READ-010621/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the the handling of app.media objects. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-13333. **CVE ID : CVE-2021-31461**	port/security-bulletins.php	
getdata_project					
getdata					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	7.5	A heap memory corruption problem (use after free) can be triggered in libgetdata v0.10.0 when processing maliciously crafted dirfile databases. This degrades the confidentiality, integrity and availability of third-party software that uses libgetdata as a library. This vulnerability may lead to arbitrary code execution or privilege escalation depending on input/skills of attacker. **CVE ID : CVE-2021-20204**	N/A	A-GET-GETD-010621/152
Gitlab					
gitlab					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	06-05-2021	4	An issue has been discovered in GitLab affecting all versions starting from 11.6. Pull mirror credentials are exposed that allows other maintainers to be able to view the credentials in plain-text, **CVE ID : CVE-2021-22206**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22206.json	A-GIT-GITL-010621/153
Missing Authorization	06-05-2021	4	An issue has been discovered in GitLab affecting versions starting with 13.5 up to 13.9.7. Improper permission check could allow the change of timestamp for issue creation or update. **CVE ID : CVE-2021-22208**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22208.json	A-GIT-GITL-010621/154
Incorrect Authorization	06-05-2021	5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.8. GitLab was not properly validating authorisation tokens which resulted in GraphQL mutation being executed. **CVE ID : CVE-2021-22209**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22209.json	A-GIT-GITL-010621/155
Allocation of Resources Without Limits or Throttling	06-05-2021	5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.2. When querying the repository branches through API, GitLab was ignoring a query parameter and returning a considerable amount of results. **CVE ID : CVE-2021-22210**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22210.json	A-GIT-GITL-010621/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	06-05-2021	3.5	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7. GitLab Dependency Proxy, under certain circumstances, can impersonate a user resulting in possibly incorrect access handling. **CVE ID : CVE-2021-22211**	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22211.json	A-GIT-GITL-010621/157
gnuplot_project					
gnuplot					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	03-05-2021	7.5	The gnuplot package prior to version 0.1.0 for Node.js allows code execution via shell metacharacters in Gnuplot commands. **CVE ID : CVE-2021-29369**	https://github.com/rkesters/gnuplot/commit/23671d4d3d28570fb19a936a6328bfac742410de	A-GNU-GNUP-010621/158
Google					
cloud_iot_device_sdk_for_embedded_c					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-05-2021	4.6	In IoT Devices SDK, there is an implementation of calloc() that doesn't have a length check. An attacker could pass in memory objects larger than the buffer and wrap around to have a smaller buffer than required, allowing the attacker access to the other parts of the heap. We recommend upgrading the Google Cloud IoT Device SDK for Embedded C used to 1.0.3 or greater. **CVE ID : CVE-2021-22547**	https://github.com/GoogleCloudPlatform/iot-device-sdk-embedded-c/blob/master/RELEASE-NOTES.md, https://github.com/GoogleCloudPlatform/iot-device-sdk-embedded-c/pull/119	A-GOO-CLOU-010621/159
handlebarsjs					
handlebars					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	04-05-2021	7.5	The package handlebars before 4.7.7 are vulnerable to Prototype Pollution when selecting certain compiling options to compile templates coming from an untrusted source. **CVE ID : CVE-2021-23383**	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1279032, https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1279031, https://github.com/handlebars-lang/handlebars.js/commit/f0589701698268578199be25285b2ebea1c1e427, https://snyk.io/vuln/SNYK-JS-HANDLEBARS-1279029	A-HAN-HAND-010621/160
hashicorp					
vault-action					
Insertion of Sensitive Information into Log File	07-05-2021	5	HashiCorp vault-action (aka Vault GitHub Action) before 2.2.0 allows attackers to obtain sensitive information from log files because a multi-line secret was not correctly registered with GitHub Actions for log masking. **CVE ID : CVE-2021-32074**	https://github.com/hashicorp/vault-action/pull/208, https://discuss.hashicorp.com/t/hcsec-2021-13-vault-github-action-did-not-	A-HAS-VAUL-010621/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				correctly-mask-multi-line-secrets-in-output/24128	
hasthemes					
ht_mega_-_absolute_addons_for_elementor_page_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "HT Mega – Absolute Addons for Elementor Page Builder" WordPress Plugin before 1.5.7 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24261**	https://wpscan.com/vulnerability/0377705d-29e9-47db-a5bb-8acaf311a38f	A-HAS-HT_M-010621/162
woolentor_-_woocommerce_elementor_addons_\\+_builder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "WooLentor – WooCommerce Elementor Addons + Builder" WordPress Plugin before 1.8.6 has a widget that is vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24262**	https://wpscan.com/vulnerability/d6d16357-2bc3-4053-8274-d0275026e56b	A-HAS-WOOL-010621/163
highcharts					
highcharts					
Improper Neutralization of Input During Web Page Generation	05-05-2021	3.5	Highcharts JS is a JavaScript charting library based on SVG. In Highcharts versions 8 and earlier, the chart options structure was not systematically filtered for XSS vectors. The potential	https://github.com/highcharts/highcharts/security/advisories/GHSA-	A-HIG-HIGH-010621/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			impact was that content from untrusted sources could execute code in the end user's browser. The vulnerability is patched in version 9. As a workaround, implementers who are not able to upgrade may apply DOMPurify recursively to the options structure to filter out malicious markup. **CVE ID : CVE-2021-29489**	8j65-4pcq-xq95	
HP					
edgeline_infrastructure_manager					
Improper Authentication	06-05-2021	10	A security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software, prior to version 1.22. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of arbitrary commands, gaining privileged access, causing denial of service, and changing the configuration. HPE has released a software update to resolve the vulnerability in the HPE Edgeline Infrastructure Manager. **CVE ID : CVE-2021-29203**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn04124en_us	A-HP-EDGE-010621/165
IBM					
cloud_pak_for_security					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	10-05-2021	6.4	IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 could allow a user to obtain sensitive information or perform actions they should not have access to due to incorrect authorization mechanisms. IBM X-Force ID: 198919. **CVE ID : CVE-2021-20538**	https://exchange.xforce.ibmcloud.com/vulnerabilities/198919, https://www.ibm.com/support/pages/node/6450849	A-IBM-CLOU-010621/166
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-05-2021	4.3	IBM Cloud Pak for Security (CP4S) 1.5.0.0 and 1.5.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 199281. **CVE ID : CVE-2021-20577**	https://www.ibm.com/support/pages/node/6450849, https://exchange.xforce.ibmcloud.com/vulnerabilities/199281	A-IBM-CLOU-010621/167
control_desk					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-05-2021	3.5	IBM Control Desk 7.6.1.2 and 7.6.1.3 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: 199228. **CVE ID : CVE-2021-20559**	https://www.ibm.com/support/pages/node/6450759, https://exchange.xforce.ibmcloud.com/vulnerabilities/199228	A-IBM-CONT-010621/168
qradar_security_information_and_event_manager					
Improper Neutralization of Input	05-05-2021	4.3	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This	https://exchange.xforce.ibmcloud.co	A-IBM-QRAD-010621/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 196017. **CVE ID : CVE-2021-20397**	m/vulnerabilities/196017, https://www.ibm.com/support/pages/node/6449688	
Use of Hard-coded Credentials	05-05-2021	4.6	IBM QRadar SIEM 7.3 and 7.4 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 196075. **CVE ID : CVE-2021-20401**	https://exchange.xforce.ibmcloud.com/vulnerabilities/196075, https://www.ibm.com/support/pages/node/6449682	A-IBM-QRAD-010621/170
ideabox					
powerpack_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Elementor Addons – PowerPack Addons for Elementor" WordPress Plugin before 2.3.2 for WordPress has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24263**	https://wpscan.com/vulnerability/48876006-b00f-49b7-80a1-b1d6dc2f4eec	A-IDE-POWE-010621/171
igt\\+_project					
imagely					
nextgen_gallery					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	4.3	In the eCommerce module of the NextGEN Gallery Pro WordPress plugin before 3.1.11, there is an action to call get_cart_items via photocrati_ajax , after that the settings[shipping_address][name] is able to inject malicious javascript. **CVE ID : CVE-2021-24293**	https://www.imagely.com/wordpress-gallery-plugin/nextgen-pro/changelog/, https://wpscan.com/vulnerability/5e1a4725-3d20-44b0-8a35-bbf4263957f7	A-IMA-NEXT-010621/172
imagements_project					
imagements					
Unrestricted Upload of File with Dangerous Type	06-05-2021	7.5	The Imagements WordPress plugin through 1.2.5 allows images to be uploaded in comments, however only checks for the Content-Type in the request to forbid dangerous files. This allows unauthenticated attackers to upload arbitrary files by using a valid image Content-Type along with a PHP filename and code, leading to RCE. **CVE ID : CVE-2021-24236**	https://wpscan.com/vulnerability/8f24e74f-60e3-4100-9ab2-ec31b9c9cdea	A-IMA-IMAG-010621/173
jellyfin					
jellyfin					
Server-Side Request Forgery (SSRF)	06-05-2021	5	Jellyfin is a free software media system that provides media from a dedicated server to end-user devices via multiple apps. Verions prior to 10.7.3 vulnerable to unauthenticated Server-	https://github.com/jellyfin/jellyfin/security/advisories/GH	A-JEL-JELL-010621/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Side Request Forgery (SSRF) attacks via the imageUrl parameter. This issue potentially exposes both internal and external HTTP servers or other resources available via HTTP `GET` that are visible from the Jellyfin server. The vulnerability is patched in version 10.7.3. As a workaround, disable external access to the API endpoints `/Items/*/RemoteImages/Download`, `/Items/RemoteSearch/Image` and `/Images/Remote` via reverse proxy, or limit to known-friendly IPs. **CVE ID : CVE-2021-29490**	SA-rgjw-4fwc-9v96	
Jenkins					
credentials					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	4.3	Jenkins Credentials Plugin 2.3.18 and earlier does not escape user-controlled information on a view it provides, resulting in a reflected cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2021-21648**	https://www.jenkins.io/security/advisory/2021-05-11/#SECURITY-2349	A-JEN-CRED-010621/175
dashboard_view					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	3.5	Jenkins Dashboard View Plugin 2.15 and earlier does not escape URLs referenced in Image Dashboard Portlets, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with	https://www.jenkins.io/security/advisory/2021-05-11/#SECURITY-2233	A-JEN-DASH-010621/176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			View/Configure permission. **CVE ID : CVE-2021-21649**		
Jetbrains					
intellij_idea					
Uncontrolled Resource Consumption	11-05-2021	5	In JetBrains IntelliJ IDEA before 2021.1, DoS was possible because of unbounded resource allocation. **CVE ID : CVE-2021-30504**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-INTE-010621/177
teamcity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	4.3	In JetBrains TeamCity before 2020.2.2, XSS was potentially possible on the test history page. **CVE ID : CVE-2021-31904**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/178
N/A	11-05-2021	4	In JetBrains TeamCity before 2020.2.2, audit logs were not sufficient when an administrator uploaded a file. **CVE ID : CVE-2021-31906**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/179
Incorrect Permission	11-05-2021	5	In JetBrains TeamCity before 2020.2.2,	https://blog.jetbrains.co	A-JET-TEAM-010621/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assignment for Critical Resource			permission checks for changing TeamCity plugins were implemented improperly. **CVE ID : CVE-2021-31907**	m/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	3.5	In JetBrains TeamCity before 2020.2.3, stored XSS was possible on several pages. **CVE ID : CVE-2021-31908**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/181
Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')	11-05-2021	7.5	In JetBrains TeamCity before 2020.2.3, argument injection leading to remote code execution was possible. **CVE ID : CVE-2021-31909**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/182
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	4.3	In JetBrains TeamCity before 2020.2.3, reflected XSS was possible on several pages. **CVE ID : CVE-2021-31911**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-05-2021	3.5	In JetBrains TeamCity before 2020.2.2, stored XSS on a tests page was possible. **CVE ID : CVE-2021-3315**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-TEAM-010621/184
youtrack					
Exposure of Sensitive Information to an Unauthorized Actor	11-05-2021	5	In JetBrains YouTrack before 2020.6.8801, information disclosure in an issue preview was possible. **CVE ID : CVE-2021-31905**	https://blog.jetbrains.com/blog/2021/05/07/jetbrains-security-bulletin-q1-2021/, https://blog.jetbrains.com	A-JET-YOUT-010621/185
juhnetec					
enterprise_resource_planning_point_of_sale_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	3.5	Special characters of ERP POS customer profile page are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks, additionally access and manipulate customer's information. **CVE ID : CVE-2021-30170**	N/A	A-JUH-ENTE-010621/186
Improper Neutralization of Input During Web	07-05-2021	3.5	Special characters of ERP POS news page are not filtered in users' input, which allow remote	N/A	A-JUH-ENTE-010621/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			authenticated attackers can inject malicious JavaScript and carry out stored XSS (Stored Cross-site scripting) attacks, additionally access and manipulate customer's information. **CVE ID : CVE-2021-30171**		
junhetec					
omnidirectional_communication_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	3.5	Special characters of picture preview page in the Quan-Fang-Wei-Tong-Xun system are not filtered in users' input, which allow remote authenticated attackers can inject malicious JavaScript and carry out Reflected XSS (Cross-site scripting) attacks, additionally access and manipulate customer's information. **CVE ID : CVE-2021-30172**	N/A	A-JUN-OMNI-010621/188
kennnyshiwa-cogs_project					
kennnyshiwa-cogs					
Improper Control of Generation of Code ('Code Injection')	06-05-2021	6.5	Kennnyshiwa-cogs contains cogs for Red Discordbot. An RCE exploit has been found in the Tickets module of kennnyshiwa-cogs. This exploit allows discord users to craft a message that can reveal sensitive and harmful information. Users can upgrade to version 5a84d60018468e5c0346f7ee74b2b4650a6dade7 to	https://github.com/kennnyshiwa/kennnyshiwa-cogs/security/advisories/GHSA-f4j2-2cwr-h473	A-KEN-KENN-010621/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			receive a patch or, as a workaround, unload tickets to render the exploit unusable. **CVE ID : CVE-2021-29493**		
leap13					
premium_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Premium Addons for Elementor" WordPress Plugin before 4.2.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24257**	https://wpscan.com/vulnerability/4ad8314e-1cbe-4642-b4ee-aac2060f9a25	A-LEA-PREM-010621/190
Libreoffice					
libreoffice					
N/A	03-05-2021	9.3	In the LibreOffice 7-1 series in versions prior to 7.1.2, and in the 7-0 series in versions prior to 7.0.5, the denylist can be circumvented by manipulating the link so it doesn't match the denylist but results in ShellExecute attempting to launch an executable type. **CVE ID : CVE-2021-25631**	https://www.libreoffice.org/about-us/security/advisories/cve-2021-25631/	A-LIB-LIBR-010621/191
livemeshelementor					
addons_for_elementor					
Improper Neutralization of Input During Web Page Generation	05-05-2021	3.5	The "Livemesh Addons for Elementor" WordPress Plugin before 6.8 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users	https://wpscan.com/vulnerability/fa6c7c7c-1027-4fa9-bb55-	A-LIV-ADDO-010621/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			such as contributors, all via a similar method. **CVE ID : CVE-2021-24260**	07ae2bb7f021	
livinglogic					
xist4c					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	4.3	LivingLogic XIST4C before 0.107.8 allows XSS via feedback.htm or feedback.wihtm. **CVE ID : CVE-2021-26122**	N/A	A-LIV-XIST-010621/193
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	4.3	LivingLogic XIST4C before 0.107.8 allows XSS via login.htm, login.wihtm, or login-form.htm. **CVE ID : CVE-2021-26123**	N/A	A-LIV-XIST-010621/194
mixme_project					
mixme					
Improper Control of Dynamically-Managed Code Resources	06-05-2021	5.5	Mixme is a library for recursive merging of Javascript objects. In Node.js mixme v0.5.0, an attacker can add or alter properties of an object via 'proto' through the mutate() and merge() functions. The polluted attribute will be directly assigned to every object in the program. This will put the availability of the program at risk causing a potential denial of service (DoS). The problem is corrected starting with version 0.5.1; no	https://github.com/adaltas/node-mixme/security/advisories/GHSA-79jw-6wg7-r9g4	A-MIX-MIXM-010621/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			workarounds are known to exist. **CVE ID : CVE-2021-29491**		
mooveagency					
contact_form_check_tester					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	3.5	The Contact Form Check Tester WordPress plugin through 1.0.2 settings are visible to all registered users in the dashboard and are lacking any sanitisation. As a result, any registered user, such as subscriber, can leave an XSS payload in the plugin settings, which will be triggered by any user visiting them, and could allow for privilege escalation. The vendor decided to close the plugin. **CVE ID : CVE-2021-24247**	https://wpscan.com/vulnerability/e2990a7a-d4f0-424e-b01d-ecf67cf9c9f3	A-MOO-CONT-010621/196
nim-lang					
nim					
Improper Certificate Validation	07-05-2021	5	Nim is a statically typed compiled systems programming language. In Nim standard library before 1.4.2, httpClient SSL/TLS certificate verification was disabled by default. Users can upgrade to version 1.4.2 to receive a patch or, as a workaround, set "verifyMode = CVerifyPeer" as documented. **CVE ID : CVE-2021-29495**	https://github.com/nim-lang/security/security/advisories/GHSA-9vqv-2jj9-7mqr	A-NIM-NIM-010621/197
NSA					
emissary					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	4.3	A Cross-site scripting (XSS) vulnerability in the DocumentAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows remote attackers to inject arbitrary web script or HTML via the uuid parameter. **CVE ID : CVE-2021-32092**	N/A	A-NSA-EMIS-010621/198
Missing Authorization	07-05-2021	4	The ConfigFileAction component of U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to read arbitrary files via the ConfigName parameter. **CVE ID : CVE-2021-32093**	N/A	A-NSA-EMIS-010621/199
Unrestricted Upload of File with Dangerous Type	07-05-2021	6.5	U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to upload arbitrary files. **CVE ID : CVE-2021-32094**	N/A	A-NSA-EMIS-010621/200
Missing Authorization	07-05-2021	5.5	U.S. National Security Agency (NSA) Emissary 5.9.0 allows an authenticated user to delete arbitrary files. **CVE ID : CVE-2021-32095**	N/A	A-NSA-EMIS-010621/201
Octobercms					
october					
Missing Authorization	03-05-2021	4.4	October is a free, open-source, self-hosted CMS platform based on the Laravel PHP Framework. A bypass of CVE-2020-26231 (fixed in 1.0.470/471 and 1.1.1) was discovered that has the same impact as	https://github.com/octobercms/october/security/advisories/GHSA-fcr8-6q7r-m4wg	A-OCT-OCTO-010621/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-26231 & CVE-2020-15247. An authenticated backend user with the `cms.manage_pages`, `cms.manage_layouts`, or `cms.manage_partials` permissions who would **normally** not be permitted to provide PHP code to be executed by the CMS due to `cms.enableSafeMode` being enabled is able to write specific Twig code to escape the Twig sandbox and execute arbitrary PHP. This is not a problem for anyone that trusts their users with those permissions to normally write & manage PHP within the CMS by not having `cms.enableSafeMode` enabled, but would be a problem for anyone relying on `cms.enableSafeMode` to ensure that users with those permissions in production do not have access to write & execute arbitrary PHP. Issue has been patched in Build 472 (v1.0.472) and v1.1.2. As a workaround, apply https://github.com/octobercms/october/commit/f63519ff1e8d375df30deba63156a2fc97aa9ee7 to your installation manually if unable to upgrade to Build 472 or v1.1.2. **CVE ID : CVE-2021-21264**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Open-emr					
openemr					
Incorrect Permission Assignment for Critical Resource	07-05-2021	6.4	The Patient Portal of OpenEMR 5.0.2.1 is affected by a incorrect access control system in portal/patient/_machine_config.php. To exploit the vulnerability, an unauthenticated attacker can register an account, bypassing the permission check of this portal's API. Then, the attacker can then manipulate and read data of every registered patient. **CVE ID : CVE-2021-32101**	https://community.open-emr.org/t/openemr-5-0-2-patch-5-has-been-released/15431	A-OPE-OPEN-010621/203
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-05-2021	6.5	A SQL injection vulnerability exists (with user privileges) in library/custom_template/ajax_code.php in OpenEMR 5.0.2.1. **CVE ID : CVE-2021-32102**	https://community.open-emr.org/t/openemr-5-0-2-patch-5-has-been-released/15431, https://www.open-emr.org/wiki/index.php/Old_Outdated_OpenEMR_Patches	A-OPE-OPEN-010621/204
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	3.5	A Stored XSS vulnerability in interface/usergroup/usergroup_admin.php in OpenEMR before 5.0.2.1 allows a admin authenticated user to inject arbitrary web script or	https://community.open-emr.org/t/openemr-5-0-2-patch-5-has-been-released/15431	A-OPE-OPEN-010621/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML via the lname parameter. **CVE ID : CVE-2021-32103**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-05-2021	6.5	A SQL injection vulnerability exists (with user privileges) in interface/forms/eye_mag/save.php in OpenEMR 5.0.2.1. **CVE ID : CVE-2021-32104**	https://community.open-emr.org/t/openemr-5-0-2-patch-5-has-been-released/15431, https://www.open-emr.org/wiki/index.php/Old_Outdated_OpenEMR_Patches	A-OPE-OPEN-010621/206
openmptcprouter					
openmptcprouter					
Improper Authentication	06-05-2021	4.3	omr-admin.py in openmptcprouter-vps-admin 0.57.3 and earlier compares the user provided password with the original password in a length dependent manner, which allows remote attackers to guess the password via a timing attack. **CVE ID : CVE-2021-31245**	https://www.openmptcprouter.com/, https://github.com/Ysurac/openmptcprouter-vps-admin/commit/a01cbc8c3d3b8bb7720bf3ff234671b4c0e1859c#diff-b89ee68e63302a732d4bde35eb04a205b06f1611147e139642	A-OPE-OPEN-010621/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				356f173195ab80	
Opensuse					
factory					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**	https://bugzilla.suse.com/show_bug.cgi?id=1184161	A-OPE-FACT-010621/208
Incorrect Default Permissions	05-05-2021	7.2	A Incorrect Default Permissions vulnerability in the packaging of virtualbox of openSUSE Factory allows local attackers in the vboxusers groupu to escalate to root. This issue affects: openSUSE Factory	https://bugzilla.suse.com/show_bug.cgi?id=1182918	A-OPE-FACT-010621/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			virtualbox version 6.1.20-1.1 and prior versions. **CVE ID : CVE-2021-25319**		
path-parse_project					
path-parse					
N/A	04-05-2021	5	All versions of package path-parse are vulnerable to Regular Expression Denial of Service (ReDoS) via splitDeviceRe, splitTailRe, and splitPathRe regular expressions. ReDoS exhibits polynomial worst-case time complexity. **CVE ID : CVE-2021-23343**	N/A	A-PAT-PATH-010621/210
posimyth					
the_plus_addons_for_elementor_page_builder_lite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "The Plus Addons for Elementor Page Builder Lite" WordPress Plugin before 2.0.6 has four widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24266**	https://wpscan.com/vulnerability/78014ddd-1cc2-4723-8194-4bf478888578	A-POS-THE_-010621/211
purethemes					
workscout					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	3.5	The Workscout Core WordPress plugin before 1.3.4, used by the WorkScout Theme did not sanitise the chat messages sent via the workscout_send_message_chat AJAX action, leading to Stored Cross-Site Scripting	https://wpscan.com/vulnerability/2365a9d0-f6f4-4602-9804-5af23d0cb11d	A-PUR-WORK-010621/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Cross-Frame Scripting issues **CVE ID : CVE-2021-24246**		
workscout_core					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	3.5	The Workscout Core WordPress plugin before 1.3.4, used by the WorkScout Theme did not sanitise the chat messages sent via the workscout_send_message_chat AJAX action, leading to Stored Cross-Site Scripting and Cross-Frame Scripting issues **CVE ID : CVE-2021-24246**	https://wpscan.com/vulnerability/2365a9d0-f6f4-4602-9804-5af23d0cb11d	A-PUR-WORK-010621/213
Python					
python					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-05-2021	4.3	The "origin" parameter passed to some of the endpoints like '/trigger' was vulnerable to XSS exploit. This issue affects Apache Airflow versions <1.10.15 in 1.x series and affects 2.0.0 and 2.0.1 and 2.x series. This is the same as CVE-2020-13944 & CVE-2020-17515 but the implemented fix did not fix the issue completely. Update to Airflow 1.10.15 or 2.0.2. Please also update your Python version to the latest available PATCH releases of the installed MINOR versions, example update to Python 3.6.13 if you are on Python 3.6. (Those contain the fix for CVE-2021-23336	https://lists.apache.org/thread.html/ra8ce70088ba291f358e077cafdb14d174b7a1ce9a9d86d1b332d6367%40%3Cusers.airflow.apache.org%3E, https://lists.apache.org/thread.html/rc005f4de9d9b0ba943ceb8ff5a21a5c6ff8a9df52632476698d99432@%3Cannounce	A-PYT-PYTH-010621/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://nvd.nist.gov/vuln/detail/CVE-2021-23336). **CVE ID : CVE-2021-28359**	.apache.org%3E	
Improper Input Validation	06-05-2021	7.5	Improper input validation of octal strings in Python stdlib ipaddress 3.10 and below allows unauthenticated remote attackers to perform indeterminate SSRF, RFI, and LFI attacks on many programs that rely on Python stdlib ipaddress. IP address octects are left stripped instead of evaluated as valid IP addresses. **CVE ID : CVE-2021-29921**	https://github.com/python/cpython/pull/25099, https://python-security.readthedocs.io/vuln/ipaddress-ipv4-leading-zeros.html, https://github.com/python/cpython/pull/12577, https://docs.python.org/3/library/ipaddress.html, https://bugs.python.org/issue36384	A-PYT-PYTH-010621/215
remotemouse					
emote_remote_mouse					
Missing Authorization	07-05-2021	5	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can maximize or minimize the window of a running process by sending the process name in a crafted packet. This information is sent in cleartext and is not protected by any authentication logic.	N/A	A-REM-EMOT-010621/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27569		
Missing Authorization	07-05-2021	5	An issue was discovered in Emote Remote Mouse through 3.015. Attackers can close any running process by sending the process name in a specially crafted packet. This information is sent in cleartext and is not protected by any authentication logic. **CVE ID : CVE-2021-27570**	N/A	A-REM-EMOT-010621/217
Missing Authorization	07-05-2021	5	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Attackers can retrieve recently used and running applications, their icons, and their file paths. This information is sent in cleartext and is not protected by any authentication logic. **CVE ID : CVE-2021-27571**	N/A	A-REM-EMOT-010621/218
Missing Authorization	07-05-2021	7.5	An issue was discovered in Emote Remote Mouse through 4.0.0.0. Remote unauthenticated users can execute arbitrary code via crafted UDP packets with no prior authorization or authentication. **CVE ID : CVE-2021-27573**	N/A	A-REM-EMOT-010621/219
Download of Code Without Integrity Check	07-05-2021	6.8	An issue was discovered in Emote Remote Mouse through 4.0.0.0. It uses cleartext HTTP to check, and request, updates. Thus, attackers can machine-in-the-middle a victim to download a malicious binary in place of the real	N/A	A-REM-EMOT-010621/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update, with no SSL errors or warnings. **CVE ID : CVE-2021-27574**		
Samba					
samba					
Out-of-bounds Read	05-05-2021	5.5	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity. **CVE ID : CVE-2021-20254**	https://www.samba.org/samba/security/CVE-2021-20254.html	A-SAM-SAMB-010621/221
secureauth					
impacket					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-05-2021	7.5	Multiple path traversal vulnerabilities exist in smbserver.py in Impacket through 0.9.22. An attacker that connects to a running smbserver instance can list and write to arbitrary files via ../ directory traversal. This could potentially be abused to achieve arbitrary code execution by	https://github.com/SecureAuthCorp/impacket/commit/49c643bf66620646884ed141c94e5fdd85bcdd2f	A-SEC-IMPA-010621/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			replacing /etc/shadow or an SSH authorized key. **CVE ID : CVE-2021-31800**		
sinaextra					
sina_extension_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The "Sina Extension for Elementor" WordPress Plugin before 3.3.12 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24269**	https://wpscan.com/vulnerability/df953a91-f1d8-42e9-8966-f2012d4f97c9	A-SIN-SINA-010621/223
Solarwinds					
serv-u_file_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	4.3	SolarWinds Serv-U before 15.2 is affected by Cross Site Scripting (XSS) via the HTTP Host header. **CVE ID : CVE-2021-25179**	https://documentation.solarwinds.com/en/success_center/servu/content/release_notes/servu_15-2_release_notes.htm	A-SOL-SERV-010621/224
stacklift					
localstack					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	07-05-2021	10	The dashboard component of StackLift LocalStack 0.12.6 allows attackers to inject arbitrary shell commands via the functionName parameter. **CVE ID : CVE-2021-32090**	N/A	A-STA-LOCA-010621/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-05-2021	4.3	A Cross-site scripting (XSS) vulnerability exists in StackLift LocalStack 0.12.6. **CVE ID : CVE-2021-32091**	N/A	A-STA-LOCA-010621/226
stormshield					
network_security					
Uncontrolled Resource Consumption	06-05-2021	5	Stormshield SNS with versions before 3.7.18, 3.11.6 and 4.1.6 has a memory-management defect in the SNMP plugin that can lead to excessive consumption of memory and CPU resources, and possibly a denial of service. **CVE ID : CVE-2021-28665**	https://advisories.stormshield.eu/	A-STO-NETW-010621/227
strapi					
strapi					
Weak Password Recovery Mechanism for Forgotten Password	06-05-2021	5.5	In Strapi through 3.6.0, the admin panel allows the changing of one's own password without entering the current password. An attacker who gains access to a valid session can use this to take over an account by changing the password. **CVE ID : CVE-2021-28128**	https://strapi.io/changelog	A-STR-STRA-010621/228
strategy11					
business_directory_plugin_-_easy_listing_directories					
Cross-Site Request Forgery (CSRF)	06-05-2021	6.8	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11.1 suffered from Cross-Site Request Forgery	https://wpscan.com/vulnerability/700f3b04-8298-447c-8d3c-	A-STR-BUSI-010621/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issues, allowing an attacker to make a logged in administrator add, edit or delete form fields, which could also lead to Stored Cross-Site Scripting issues. **CVE ID : CVE-2021-24178**	4581880a63b5	
Cross-Site Request Forgery (CSRF)	06-05-2021	6.8	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator import files. As the plugin also did not validate uploaded files, it could lead to RCE. **CVE ID : CVE-2021-24179**	https://wpscan.com/vulnerability/c0a5cdde-732a-432a-86c2-776df5d130a7	A-STR-BUSI-010621/230
Cross-Site Request Forgery (CSRF)	06-05-2021	4.3	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator export files, which could then be downloaded by the attacker to get access to PII, such as email, home addresses etc **CVE ID : CVE-2021-24249**	https://wpscan.com/vulnerability/fc4cf749-34ef-43b8-a529-5065d698ab81	A-STR-BUSI-010621/231
Improper Neutralization of Input During Web Page Generation	06-05-2021	3.5	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from lack of sanitisation in the label of the Form Fields, leading to	https://wpscan.com/vulnerability/e23bf712-d891-4df7-99cc-	A-STR-BUSI-010621/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Authenticated Stored Cross-Site Scripting issues across various pages of the plugin. **CVE ID : CVE-2021-24250**	9ef64f19f685	
easy_listing_directories					
Unrestricted Upload of File with Dangerous Type	06-05-2021	6.5	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11.1 did not properly check for imported files, forbidding certain extension via a blacklist approach, allowing administrator to import an archive with a .php4 inside for example, leading to RCE **CVE ID : CVE-2021-24248**	https://wpscan.com/vulnerability/ca886a34-cd2b-4032-9de1-8089b5cf3001	A-STR-EASY-010621/233
Cross-Site Request Forgery (CSRF)	06-05-2021	4.3	The Business Directory Plugin â€“ Easy Listing Directories for WordPress WordPress plugin before 5.11.2 suffered from a Cross-Site Request Forgery issue, allowing an attacker to make a logged in administrator update arbitrary payment history, such as change their status (from pending to completed to example) **CVE ID : CVE-2021-24251**	https://wpscan.com/vulnerability/c9911236-4af3-4557-9bc0-217face534e1	A-STR-EASY-010621/234
supsystic					
contact_form					
Improper Neutralization of Input During Web Page Generation	05-05-2021	4.3	The Contact Form by Supsystic WordPress plugin before 1.7.15 did not sanitise the tab parameter of its options page before outputting it in an	https://wpscan.com/vulnerability/1301123c-5e63-432a-ab90-	A-SUP-CONT-010621/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			attribute, leading to a reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24276**	3221ca532d9c	
popup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	4.3	The Popup by Supsystic WordPress plugin before 1.10.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24275**	https://wpscan.com/vulnerability/efdc76e0-c14a-4baf-af70-9d381107308f	A-SUP-POPU-010621/236
ultimate_maps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	4.3	The Ultimate Maps by Supsystic WordPress plugin before 1.2.5 did not sanitise the tab parameter of its options page before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue **CVE ID : CVE-2021-24274**	https://wpscan.com/vulnerability/200a3031-7c42-4189-96b1-bed9e0ab7c1d	A-SUP-ULTI-010621/237
Suse					
cups					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the	https://bugzilla.suse.com/show_bug.cgi?id=1184161	A-SUS-CUPS-010621/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**		
manager_server					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version	https://bugzilla.suse.com/show_bug.cgi?id=1184161	A-SUS-MANA-010621/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**		
openstack_cloud_crowbar					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**	https://bugzilla.suse.com/show_bug.cgi?id=1184161	A-SUS-OPEN-010621/240
themesgrove					
all-in-one_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation	05-05-2021	3.5	The “All-in-One Addons for Elementor – WidgetKit” WordPress Plugin before 2.3.10 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged	https://wpscan.com/vulnerability/0c96f3a1-d192-481f-9035-	A-THE-ALL--010621/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			users such as contributors, all via a similar method. **CVE ID : CVE-2021-24267**	5393f4aadc19	
Trendmicro					
home_network_security					
N/A	05-05-2021	7.8	Trend Micro Home Network Security 6.5.599 and earlier is vulnerable to a file-parsing vulnerability which could allow an attacker to exploit the vulnerability and cause a denial-of-service to the device. This vulnerability is similar, but not identical to CVE-2021-31518. **CVE ID : CVE-2021-31517**	https://helpcenter.trendmicro.com/en-us/article/TMKA-10312	A-TRE-HOME-010621/242
N/A	05-05-2021	7.8	Trend Micro Home Network Security 6.5.599 and earlier is vulnerable to a file-parsing vulnerability which could allow an attacker to exploit the vulnerability and cause a denial-of-service to the device. This vulnerability is similar, but not identical to CVE-2021-31517. **CVE ID : CVE-2021-31518**	https://helpcenter.trendmicro.com/en-us/article/TMKA-10312	A-TRE-HOME-010621/243
trumani					
stop_spammers					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	4.3	The Stop Spammers WordPress plugin before 2021.9 did not escape user input when blocking requests (such as matching a spam word), outputting it in an attribute after sanitising it to remove HTML tags, which is not sufficient and lead to a	https://wpscan.com/vulnerability/5e7accd6-08dc-4c6e-9d19-73e2d7e97735	A-TRU-STOP-010621/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reflected Cross-Site Scripting issue. **CVE ID : CVE-2021-24245**		
Vaadin					
vaadin					
Uncontrolled Resource Consumption	06-05-2021	5	Unsafe validation RegEx in EmailValidator component in com.vaadin:vaadin-compatibility-server versions 8.0.0 through 8.12.4 (Vaadin versions 8.0.0 through 8.12.4) allows attackers to cause uncontrolled resource consumption by submitting malicious email addresses. **CVE ID : CVE-2021-31409**	https://github.com/vaadin/framework/pull/12241, https://github.com/vaadin/framework/issues/12240, https://vaadin.com/security/cve-2021-31409	A-VAA-VAAD-010621/245
wayfair					
git-parse					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-05-2021	6.8	The "gitDiff" function in Wayfair git-parse <=1.0.4 has a command injection vulnerability. Clients of the git-parse library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. **CVE ID : CVE-2021-26543**	N/A	A-WAY-GIT--010621/246
webtechstreet					
elementor_addon_elements					
Improper Neutralization of Input During Web Page Generation	05-05-2021	3.5	The “Elementor Addon Elements” WordPress Plugin before 1.11.2 has several widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users	https://wpscan.com/vulnerability/0719063f-7743-4a34-94b9-	A-WEB-ELEM-010621/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			such as contributors, all via a similar method. **CVE ID : CVE-2021-24259**	f67fd98e5990	
wp-eventmanager					
event_banner					
Unrestricted Upload of File with Dangerous Type	06-05-2021	6.5	The Event Banner WordPress plugin through 1.3 does not verify the uploaded image file, allowing admin accounts to upload arbitrary files, such as .exe, .php, or others executable, leading to RCE. Due to the lack of CSRF check, the issue can also be used via such vector to achieve the same result, or via a LFI as authorisation checks are missing (but would require WP to be loaded) **CVE ID : CVE-2021-24252**	https://wpscan.com/vulnerability/91e81c6d-f24d-4f87-bc13-746715af8f7c	A-WP--EVEN-010621/248
wpbakery_page_builder_clipboard_project					
wpbakery_page_builder_clipboard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-05-2021	3.5	An AJAX action registered by the WPBakery Page Builder (Visual Composer) Clipboard WordPress plugin before 4.5.6 did not have capability checks nor sanitization, allowing low privilege users (subscriber+) to call it and set XSS payloads, which will be triggered in all backend pages. **CVE ID : CVE-2021-24243**	https://wpscan.com/vulnerability/3bc0733a-b949-40c9-a5fb-f56814fc4af3	A-WPB-WPBA-010621/249
Incorrect Authorization	06-05-2021	4	An AJAX action registered by the WPBakery Page Builder (Visual Composer) Clipboard WordPress	https://wpscan.com/vulnerability/354b98d8-	A-WPB-WPBA-010621/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			plugin before 4.5.8 did not have capability checks, allowing low privilege users, such as subscribers, to update the license options (key, email). **CVE ID : CVE-2021-24244**	46a1-4189-b347-198701ea59b9	
wpdeveloper					
essential_addons_for_elementor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	3.5	The Essential Addons for Elementor Lite WordPress Plugin before 4.5.4 has two widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, both via a similar method. **CVE ID : CVE-2021-24255**	https://wpscan.com/vulnerability/7fb708da-e8c4-4455-b4f9-c4ad72f877da	A-WPD-ESSE-010621/251
wpmet					
elements_kit_elementor_addons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-05-2021	4	The Elements Kit Lite and Elements Kit Pro WordPress Plugins before 2.2.0 have a number of widgets that are vulnerable to stored Cross-Site Scripting (XSS) by lower-privileged users such as contributors, all via a similar method. **CVE ID : CVE-2021-24258**	https://wpscan.com/vulnerability/47b47b86-899b-4de3-8a3c-2d5d1774298f	A-WPM-ELEM-010621/252
Hardware					
Asus					
gt-ac2900					
Improper Authentication	06-05-2021	7.5	The administrator application on ASUS GT-AC2900 devices before 3.0.0.4.386.42643 allows	https://www.asus.com/Networking-IoT-	H-ASU-GT-A-010621/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication bypass when processing remote input from an unauthenticated user, leading to unauthorized access to the administrator interface. This relates to handle_request in router/httpd/httpd.c and auth_check in web_hook.o. An attacker-supplied value of '\0' matches the device's default value of '\0' in some situations. **CVE ID : CVE-2021-32030**	Servers/Wifi-Routers/ASUS-Gaming-Routers/RT-AC2900/HelpDesk_BIOS/	
Cisco					
c125_m5					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C125-010621/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c220_m5					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C220-010621/255
c220_m6					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C220-010621/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c225_m6					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C225-010621/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c240_m5					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C240-010621/258
c240_m6					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C240-010621/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c245_m6					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C245-010621/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c480_m5					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C480-010621/261
c480_ml_m5					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-C480-010621/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
encs_5100					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-ENCS-010621/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
encs_5400					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-ENCS-010621/264
hyperflex_hx220c_af_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	H-CIS-HYPE-010621/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			see the Details section of this advisory. **CVE ID : CVE-2021-1497**		
hyperflex_hx220c_all_nvme_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	H-CIS-HYPE-010621/266
hyperflex_hx220c_edge_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	H-CIS-HYPE-010621/267
hyperflex_hx220c_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-	H-CIS-HYPE-010621/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	rce-TjjNrkpR	
hyperflex_hx240c					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	H-CIS-HYPE-010621/269
hyperflex_hx240c_af_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	H-CIS-HYPE-010621/270
hyperflex_hx240c_m5					
Improper Neutralization of Special Elements used in an OS Command ('OS	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-	H-CIS-HYPE-010621/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	rce-TjjNrkpR	
rv340					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	H-CIS-RV34-010621/272
rv340w					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340,	https://tools.cisco.com/security/cen	H-CIS-RV34-010621/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**	ter/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	
rv345					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	H-CIS-RV34-010621/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**		
rv345p					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	H-CIS-RV34-010621/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**		
ucs_e1120d_m3					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/276
ucs_e140d					
URL Redirection to Untrusted	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management	https://tools.cisco.com/security/center/content/	H-CIS-UCS_-010621/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	
ucs_e140dp					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e140s					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/279
ucs_e140s_m1					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software	https://tools.cisco.com/security/center/content/CiscoSecurit	H-CIS-UCS_-010621/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	yAdvisory/cisco-sa-imc-openred-zAYrU6d2	
ucs_e140s_m2					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e160d					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/282
ucs_e160dp_m1					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/c	H-CIS-UCS_-010621/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	isco-sa-imc-openred-zAYrU6d2	
ucs_e160s_m3					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e180d_m2					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/285
ucs_e180d_m3					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-	H-CIS-UCS_-010621/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	openred-zAYrU6d2	
ucs_s3260					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	H-CIS-UCS_-010621/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
vedge-100b					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/288
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/289
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-	H-CIS-VEDG-010621/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**	buffover-MWGucjtO	
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/291
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge-cloud					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/293
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/294
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/296
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_100					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/298
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/299
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/301
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_1000					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/303
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/304
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/306
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_100b					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/308
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/309
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/311
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_100m					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/313
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/314
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/316
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_100wm					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/318
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/319
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/321
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_2000					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/323
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/324
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/326
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vedge_5000					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/328
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/329
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	H-CIS-VEDG-010621/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the Details section of this advisory. **CVE ID : CVE-2021-1511**		
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VEDG-010621/331
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VEDG-010621/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
vsmart_controller					
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	H-CIS-VSMA-010621/333
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	H-CIS-VSMA-010621/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**		
hongdian					
h8922					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-05-2021	4	Hongdian H8922 3.0.5 devices allow Directory Traversal. The /log_download.cgi log export handler does not validate user input and allows a remote attacker with minimal privileges to download any file from the device by substituting ../ (e.g., ../../etc/passwd) This can be carried out with a web browser by changing the file name accordingly. Upon visiting log_download.cgi?type=../../etc/passwd and logging in, the web server will allow a download of the contents of the /etc/passwd file. **CVE ID : CVE-2021-28149**	http://en.hongdian.com/Products/Details/H8922	H-HON-H892-010621/335
Improper Input Validation	06-05-2021	2.1	Hongdian H8922 3.0.5 devices allow the unprivileged guest user to read cli.conf (with the administrator password and other sensitive data) via /backup2.cgi. **CVE ID : CVE-2021-28150**	http://en.hongdian.com/Products/Details/H8922	H-HON-H892-010621/336
Improper Neutralization of Special Elements	06-05-2021	9	Hongdian H8922 3.0.5 devices allow OS command injection via shell metacharacters into the ip-	http://en.hongdian.com/Products/Details/H8922	H-HON-H892-010621/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			address (aka Destination) field to the tools.cgi ping command, which is accessible with the username guest and password guest. **CVE ID : CVE-2021-28151**		
Use of Hard-coded Credentials	06-05-2021	7.5	Hongdian H8922 3.0.5 devices have an undocumented feature that allows access to a shell as a superuser. To connect, the telnet service is used on port 5188 with the default credentials of root:superzxmn. **CVE ID : CVE-2021-28152**	http://en.hongdian.com/Products/Details/H8922	H-HON-H892-010621/338
Qualcomm					
apq8009					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/339
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/341
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/342
apq8009w					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/344
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/345
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/346
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-APQ8-010621/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
apq8017					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/348
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/349
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-APQ8-010621/350

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/351
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/352
apq8053					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-APQ8-010621/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/354
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/355
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/357
apq8064au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/358
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/360
apq8096au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/361
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-APQ8-010621/364
aqt1000					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AQT1-010621/365
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of	https://www.qualcomm.com/compa	H-QUA-AQT1-010621/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	ny/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AQT1-010621/367
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AQT1-010621/368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-AQT1-010621/369

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AQT1-010621/370
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AQT1-010621/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
ar8031					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/372
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/373
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/374
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-AR80-010621/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/376
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/378
ar8035					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/379
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/380
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-AR80-010621/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/382
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-AR80-010621/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR80-010621/384
ar8151					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR81-010621/385
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-AR81-010621/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR81-010621/387
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR81-010621/388
ar9380					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-AR93-010621/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR93-010621/390
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-AR93-010621/391
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-AR93-010621/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
csr8811					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSR8-010621/393
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSR8-010621/394
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-CSR8-010621/395

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSR8-010621/396
csra6620					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/397
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-CSRA-010621/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/399
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/400
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/401

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/402
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/403
csra6640					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/404
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/405
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/406
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-CSRA-010621/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/408
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRA-010621/409
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-CSRA-010621/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
csrb31024					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRB-010621/411
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRB-010621/412
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-CSRB-010621/413

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRB-010621/414
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-CSRB-010621/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fsm10055					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/416
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/417
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/418
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	H-QUA-FSM1-010621/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/420
fsm10056					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/422
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-FSM1-010621/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-FSM1-010621/425
ipq4018					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/426
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ4-010621/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/428
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/429
ipq4019					
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ4-010621/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/431
ipq4028					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/432
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ4-010621/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/434
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq4029					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/436
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/437
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-IPQ4-010621/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ4-010621/439
ipq5010					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ5-010621/440
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-IPQ5-010621/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ5-010621/442
ipq5018					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ5-010621/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ5-010621/444
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ5-010621/445
ipq6000					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-IPQ6-010621/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/447
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/448
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-IPQ6-010621/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
ipq6005					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/450
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-IPQ6-010621/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/452
ipq6010					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/453
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ6-010621/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/455
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/456
ipq6018					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/457
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/458
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/460
ipq6028					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/461
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/463
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ6-010621/464
ipq8064					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/466
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/467
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8065					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/469
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/470
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8068					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/472
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/473
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8069					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/475
ipq8070					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/476
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-IPQ8-010621/477

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/478
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
ipq8070a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/480
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/481
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-IPQ8-010621/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/483
ipq8071					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ8-010621/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/486
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/487
ipq8071a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ8-010621/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/489
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/490
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ8-010621/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	letins/may-2021-bulletin	
ipq8072					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/493
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ8-010621/494

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/495
ipq8072a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/496
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-IPQ8-010621/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/498
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8074					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/500
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/501
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-IPQ8-010621/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/503
ipq8074a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ8-010621/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/506
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/507
ipq8076					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-010621/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/509
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/510
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-010621/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
ipq8076a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/513
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-IPQ8-010621/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/515
ipq8078					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-IPQ8-010621/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/517
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/518
ipq8078a					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-IPQ8-010621/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/520
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/521
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-IPQ8-010621/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
ipq8173					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/524
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group	https://www.qualcomm.com/compa	H-QUA-IPQ8-010621/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/526
ipq8174					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/527
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	H-QUA-IPQ8-010621/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/529
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-IPQ8-010621/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
mdm9150					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/531
mdm9206					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/532
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/534
mdm9250					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/535
mdm9607					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/537
mdm9626					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/538
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
mdm9628					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/540
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/541
mdm9650					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/543
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MDM9-010621/544
msm8909w					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/545
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of	https://www.qualcomm.com/compa	H-QUA-MSM8-010621/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	ny/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/547
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/548
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-MSM8-010621/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
msm8917					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/550
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/551
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/553
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/554
msm8953					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/556
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/557
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/558
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-MSM8-010621/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
msm8996au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/560
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-MSM8-010621/562
pm215					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM21-010621/563
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM21-010621/564
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM21-010621/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM21-010621/566
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM21-010621/567
pm3003a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/569
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/570
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/571
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-PM30-010621/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/573
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM30-010621/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm4125					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM41-010621/575
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM41-010621/576
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM41-010621/577
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-PM41-010621/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM41-010621/579
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-PM41-010621/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM41-010621/581
pm4250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/582
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/584
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM42-010621/587
pm439					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM43-010621/588
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM43-010621/589
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-PM43-010621/590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM43-010621/591
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM43-010621/592
pm456					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-PM45-010621/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM45-010621/594
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM45-010621/595
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM45-010621/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM45-010621/597
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM45-010621/598
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM45-010621/599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pm6125					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/600
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/601
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/603
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/604
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM61-010621/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/606
pm6150					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/607
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/609
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/610
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM61-010621/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/612
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/613
pm6150a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM61-010621/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/615
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/616
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/618
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/619
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm6150l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/621
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/622
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/625
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM61-010621/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM61-010621/627
pm6250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/628
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/630
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM62-010621/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/633
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM62-010621/634
pm6350					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM63-010621/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/636
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/637
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/639
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/640
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM63-010621/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm640a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/642
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/643
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/645
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/646
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM64-010621/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/648
pm640l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/649
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/651
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM64-010621/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/654
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/655
pm640p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM64-010621/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/657
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/658
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/660
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/661
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM64-010621/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm660					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/663
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/664
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/667
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM66-010621/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/669
pm660a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/670
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/672
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM66-010621/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/675
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/676
pm660l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM66-010621/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/678
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/679
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/681
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/682
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM66-010621/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm670					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/684
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/685
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/687
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/688
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-PM67-010621/689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm670a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/690
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/691
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/693
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/694
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm670l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/696
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/697
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/698
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-PM67-010621/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/700
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM67-010621/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pm7150a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/702
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/703
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/704
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM71-010621/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/706
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/707
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-PM71-010621/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
pm7150l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/709
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/710
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM71-010621/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/712
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/713
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM71-010621/714

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM71-010621/715
pm7250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/716
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM72-010621/717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/718
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/719
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM72-010621/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/721
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/722
pm7250b					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/723
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/724
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/725
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM72-010621/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/727
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM72-010621/728
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-PM72-010621/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
pm7350c					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM73-010621/730
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM73-010621/731
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM73-010621/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM73-010621/733
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM73-010621/734
pm8004					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM80-010621/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/736
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/737
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/739
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/740
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8005					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/742
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/743
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/745
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/746
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM80-010621/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/748
pm8008					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/749
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/751
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/752
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM80-010621/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/754
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/755
pm8009					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM80-010621/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/757
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/758
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/760
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/761
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM80-010621/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8150					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/763
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/764
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/766
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/767
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM81-010621/768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	letins/may-2021-bulletin	
pm8150a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/769
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/770
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM81-010621/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/772
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/773
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/774

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/775
pm8150b					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/776
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/778
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/779
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM81-010621/780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/781
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/782
pm8150c					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-PM81-010621/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/784
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/785
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/787
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/788
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM81-010621/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pm8150l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/790
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/791
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/793
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/794
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM81-010621/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM81-010621/796
pm8250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/797
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/799
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/800
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM82-010621/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/802
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM82-010621/803
pm8350					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM83-010621/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/805
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/806
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/808
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/809
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8350b					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/811
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/812
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/815
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM83-010621/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/817
pm8350bh					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/818
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/820
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/821
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM83-010621/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/823
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/824
pm8350bhs					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM83-010621/825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/826
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM83-010621/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/829
pm8350c					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/830
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/832
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/835
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM83-010621/836
pm855					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/838
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/839
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/840
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-PM85-010621/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/842
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm855a					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/844
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/845
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM85-010621/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/847
pm855b					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/848
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/850
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/851
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM85-010621/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/853
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/854
pm855l					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PM85-010621/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/856
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/857
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/859
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/860
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm855p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/862
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/863
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/866
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PM85-010621/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM85-010621/868
pm8909					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/869
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/871
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/872
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
pm8916					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/874
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/875
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/876
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-PM89-010621/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/878
pm8937					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/879
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/881
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/882
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8953					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/884
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/885
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/886
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-PM89-010621/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/888
pm8998					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/889
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PM89-010621/890

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/891
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PM89-010621/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/894
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PM89-010621/895
pmc1000h					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-PMC1-010621/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC1-010621/897
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC1-010621/898
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC1-010621/899

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC1-010621/900
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC1-010621/901
pmc7180					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMC7-010621/902
pmd9607					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/903
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/905
pmd9655					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/906
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/907
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure.	https://www.qualcomm.com/company/product-	H-QUA-PMD9-010621/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/909
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/910
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-PMD9-010621/911

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/912
pmd9655au					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMD9-010621/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pme605					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PME6-010621/914
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PME6-010621/915
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PME6-010621/916
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PME6-010621/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PME6-010621/918
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PME6-010621/919
pmi632					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-PMI6-010621/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI6-010621/921
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI6-010621/922
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI6-010621/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI6-010621/924
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI6-010621/925
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMI6-010621/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pmi8937					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/927
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/928
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/930
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/931
pmi8952					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/932
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of	https://www.qualcomm	H-QUA-PMI8-010621/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	.com/company/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/934
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/935
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMI8-010621/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pmi8998					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/937
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/938
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/941
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/942

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMI8-010621/943
pmk7350					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK7-010621/944
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK7-010621/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK7-010621/946
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK7-010621/947
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-PMK7-010621/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmk8002					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/949
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/950
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/953
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-PMK8-010621/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/955
pmk8003					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/956
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/958
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/961
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/962
pmk8350					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/964
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/965
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/966
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-PMK8-010621/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/968
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMK8-010621/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmm6155au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/970
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/971
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/974
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-PMM6-010621/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM6-010621/976
pmm8155au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/977
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/979
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/982
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/983
pmm8195au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/985
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/986
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/987
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-PMM8-010621/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/989
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmm855au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/991
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/992
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/994
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/995
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-PMM8-010621/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/997
pmm8920au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/998
pmm8996au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMM8-010621/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/1000
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/1001
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMM8-010621/1002

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-2021-1915**		
pmp8074					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMP8-010621/1003
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMP8-010621/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMP8-010621/1005
pmr525					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR5-010621/1006
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR5-010621/1007
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-PMR5-010621/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR5-010621/1009
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR5-010621/1010
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-PMR5-010621/1011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR5-010621/1012
pmr735a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1013
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-PMR7-010621/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1015
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1017

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1018
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pmr735b					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1020
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1021
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1022
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMR7-010621/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1024
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMR7-010621/1025
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-PMR7-010621/1026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
pmw3100					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMW3-010621/1027
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMW3-010621/1028
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMW3-010621/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMW3-010621/1030
pmx20					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1031
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-PMX2-010621/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1033
pmx24					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1034
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1036
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1037
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-PMX2-010621/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX2-010621/1039
pmx50					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1040
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1042
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-PMX5-010621/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1045
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1046
pmx55					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-PMX5-010621/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1048
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1049
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1051
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1052
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-PMX5-010621/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat3514					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1054
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1055
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1057
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1058
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QAT3-010621/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1060
qat3516					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1061
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1063
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1064
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QAT3-010621/1065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1066
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1067
qat3518					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QAT3-010621/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1069
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1070
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1072
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1073
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat3519					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1075
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1076
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1078
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1079
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QAT3-010621/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1081
qat3522					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1082
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1084
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QAT3-010621/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1087
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1088
qat3550					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QAT3-010621/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1090
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1091
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1093
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1094
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat3555					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1096
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1097
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1100
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QAT3-010621/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT3-010621/1102
qat5515					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1103
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1105
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1106
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QAT5-010621/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1108
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1109
qat5516					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QAT5-010621/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1111
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1112
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1114
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1115
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat5522					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1117
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1118
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1120
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1121
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QAT5-010621/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1123
qat5533					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1124
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1126
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1127
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QAT5-010621/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1129
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1130
qat5568					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QAT5-010621/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1132
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1133
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1135
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1136
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QAT5-010621/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qbt1000					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1138
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1139
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QBT1-010621/1140

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-2021-1925**	2021-bulletin	
qbt1500					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1141
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1142
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1144
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1145
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1146

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT1-010621/1147
qbt2000					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1148
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1150
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1151
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QBT2-010621/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1153
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QBT2-010621/1154
qca1062					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA1-010621/1155

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-2021-1925**	letins/may-2021-bulletin	
qca1064					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA1-010621/1156
qca2066					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCA2-010621/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
qca4020					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1158
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1159
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca4024					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1161
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1162
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1163

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA4-010621/1164
qca6174					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1165
qca6174a					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length	https://www.qualcomm	H-QUA-QCA6-010621/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1167
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1168
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1170
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1171
qca6175a					
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA6-010621/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1173
qca6310					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1174
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-QCA6-010621/1175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1176
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1177
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1178

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1179
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6320					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1181
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1182
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1183
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	H-QUA-QCA6-010621/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1185
qca6335					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1187
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1188
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1189
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-010621/1190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1191
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6390					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1193
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1194
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1195
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QCA6-010621/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1197
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA6-010621/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1199
qca6391					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1200
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1202
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1203
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1205
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1206
qca6420					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1208
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1209
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1210
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-010621/1211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1212
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6421					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1214
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1215
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1216
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QCA6-010621/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1218
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6426					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1220
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1221
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1222
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QCA6-010621/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1224
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA6-010621/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1226
qca6428					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1227
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA6-010621/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1229
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1230
qca6430					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA6-010621/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1232
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1233
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1235
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1236
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6431					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1238
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1239
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1241
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1242
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6436					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1244
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1245
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1247
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1248
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCA6-010621/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1250
qca6438					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1251
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA6-010621/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1253
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1254
qca6564					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1255
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1256
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1257
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA6-010621/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1259
qca6564a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1260
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1262
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1263
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA6-010621/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1265
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1266
qca6564au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA6-010621/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1268
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1269
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1271
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1272
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6574					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1274
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1275
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1278
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCA6-010621/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1280
qca6574a					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1281
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1283
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1284
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA6-010621/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1286
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1287
qca6574au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA6-010621/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1289
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1290
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1292
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1293
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6584au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1295
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1296
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1298
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1299
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA6-010621/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	letins/may-2021-bulletin	
qca6595					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1301
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1302
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCA6-010621/1303

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-2021-1925**	letins/may-2021-bulletin	
qca6595au					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1304
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1305
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA6-010621/1306

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1307
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1308
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1309

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1310
qca6694					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA6-010621/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
qca6696					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1312
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1313
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1314
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-010621/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1316
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA6-010621/1318
qca7500					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA7-010621/1319
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA7-010621/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA7-010621/1321
qca8072					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1322
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1324
qca8075					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA8-010621/1326

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1327
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca8081					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1329
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1330
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA8-010621/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1332
qca8337					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1333
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1336
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCA8-010621/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA8-010621/1338
qca9367					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1339
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1340

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1341
qca9377					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1342
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1344
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1345
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1347
qca9379					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1348
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1350
qca9531					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1351
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9558					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1353
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9561					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1355
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1356
qca9563					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1357

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-2021-1915**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1358
qca9880					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1359
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1361
qca9882					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA9-010621/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
qca9886					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1364
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9887					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1366
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1367
qca9888					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QCA9-010621/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1369
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1370
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QCA9-010621/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qca9889					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1372
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1373
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group	https://www.qualcomm.com/compa	H-QUA-QCA9-010621/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1375
qca9896					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA9-010621/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1377
qca9898					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1378
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCA9-010621/1379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1380
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1381
qca9980					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1382
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1383
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1385
qca9982					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1386
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9984					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1389
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1390

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1391
qca9985					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1393

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-2021-1915**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1394
qca9990					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1395
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCA9-010621/1396

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1397
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9992					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1399
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1400
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA9-010621/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1402
qca9994					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1403
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCA9-010621/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1405
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCA9-010621/1406
qcc1110					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCC1-010621/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCC1-010621/1408
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCC1-010621/1409
qcm2290					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1411
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1412
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1413
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QCM2-010621/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1415
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM2-010621/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcm4290					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM4-010621/1417
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM4-010621/1418
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM4-010621/1419
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QCM4-010621/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM4-010621/1421
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM4-010621/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcm6125					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM6-010621/1423
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM6-010621/1424
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM6-010621/1425
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCM6-010621/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM6-010621/1427
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCM6-010621/1428
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QCM6-010621/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcn5021					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1430
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCN5-010621/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1432
qcn5022					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1434
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1435
qcn5024					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1436

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1437
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn5052					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1439
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1440
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCN5-010621/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcn5054					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1442
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-QCN5-010621/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1444
qcn5064					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1445
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCN5-010621/1446

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1447
qcn5121					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCN5-010621/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1449
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1450
qcn5122					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QCN5-010621/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1452
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1453
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QCN5-010621/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qcn5124					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1455
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCN5-010621/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1457
qcn5152					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1458
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCN5-010621/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1460
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1461
qcn5154					
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	H-QUA-QCN5-010621/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1463
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcn5164					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1465
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1466
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QCN5-010621/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcn5500					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1468
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-QCN5-010621/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcn5502					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1470
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1471
qcn5550					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1472
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1473
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN5-010621/1475
qcn6023					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN6-010621/1476
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN6-010621/1477

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN6-010621/1478
qcn6024					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QCN6-010621/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN6-010621/1480
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN6-010621/1481
qcn7605					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCN7-010621/1482

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN7-010621/1483
qcn7606					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCN7-010621/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN7-010621/1485
qcn9000					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1486
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-QCN9-010621/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1488
qcn9012					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCN9-010621/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1490
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1491
qcn9022					
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	H-QUA-QCN9-010621/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1493
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcn9024					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1495
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1496
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QCN9-010621/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcn9070					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1498
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCN9-010621/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1500
qcn9072					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1502
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1503
qcn9074					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1504

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1505
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn9100					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1507
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCN9-010621/1508
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCN9-010621/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcs2290					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1510
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1511
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1513
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1514
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QCS2-010621/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS2-010621/1516
qcs405					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1517
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1519
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1520
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QCS4-010621/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1522
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1523
qcs410					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QCS4-010621/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1525
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1526
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1528
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1529
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcs4290					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1531
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1532
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1534
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS4-010621/1535
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-QCS4-010621/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcs603					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1537
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1538
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1540
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1541
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcs605					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1543
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1544
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1545
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QCS6-010621/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1547
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcs610					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1549
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1550
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1551
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCS6-010621/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1553
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1554
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QCS6-010621/1555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcs6125					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1556
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1557
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCS6-010621/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1559
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1560
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QCS6-010621/1561

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QCS6-010621/1562
qdm2301					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1563
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1565
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1566
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QDM2-010621/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1568
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1569
qdm2302					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1570
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1571
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1572
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1574
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1575
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QDM2-010621/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qdm2305					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1577
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1578
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1579

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1581
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1582

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1583
qdm2307					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1584
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1585

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1586
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1587
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QDM2-010621/1588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1589
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1590
qdm2308					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1591
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1592
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1593
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1595
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1596
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QDM2-010621/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qdm2310					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1598
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1599
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM2-010621/1600

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1602
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1603

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM2-010621/1604
qdm3301					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1605
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QDM3-010621/1606

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1607
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1608
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QDM3-010621/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1610
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1611
qdm3302					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1612
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1613
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1615

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-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM3-010621/1616
qdm4643					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1617
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1619
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QDM4-010621/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1622
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1623
qdm4650					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QDM4-010621/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1625
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1626
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1628
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1629
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM4-010621/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5579					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1631
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1632
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1634
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1635
qdm5620					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1637
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1638
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1639
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QDM5-010621/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1641
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5621					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1643
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1644
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1646
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1647
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-QDM5-010621/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1649
qdm5650					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1650
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1652
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1653
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1655
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1656
qdm5652					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1658
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1659
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1660
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QDM5-010621/1661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1662
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5670					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1664
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1665
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1667
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1668
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-QDM5-010621/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1670
qdm5671					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1671
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1673
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1674
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1676
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1677
qdm5677					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1679
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1680
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1681
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QDM5-010621/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1683
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5679					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1685
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1686
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1688
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1689
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-QDM5-010621/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QDM5-010621/1691
qet4100					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1692
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1694
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1695
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1697
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1698
qet4101					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1700
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1701
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1702
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QET4-010621/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1704
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qet4200aq					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET4-010621/1706
qet5100					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1707
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1709
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QET5-010621/1711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1712
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1713
qet5100m					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QET5-010621/1714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1715
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1716
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1718
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1719
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET5-010621/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qet6100					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1721
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1722
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1724
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1725
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QET6-010621/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1727
qet6105					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1728
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1730
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QET6-010621/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1733
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1734
qet6110					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QET6-010621/1735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1736
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1737
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1739
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1740
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QET6-010621/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe2080fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1742
qfe2081fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QFE2-010621/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
qfe2082fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1744
qfe2101					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1745
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1747
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1748
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1750
qfe2520					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1751
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1752
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-QFE2-010621/1753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1754
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1755
qfe2550					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QFE2-010621/1756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1757
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1758
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE2-010621/1760
qfe3100					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1761
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1762

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-2021-1925**		
qfe3340					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1763
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1764
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1766
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE3-010621/1767
qfe3440fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QFE3-010621/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
qfe4301					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1769
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1770
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1772
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1773
qfe4302					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1774
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-QFE4-010621/1775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1776
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1777
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe4303					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1779
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1780
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1782
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1783
qfe4305					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1784
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of	https://www.qualcomm	H-QUA-QFE4-010621/1785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	.com/company/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1786
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1787
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QFE4-010621/1788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qfe4308					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1789
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1790
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1792
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1793
qfe4309					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1795
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1796
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1797
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QFE4-010621/1798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qfe4320					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1799
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1800
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QFE4-010621/1801

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1802
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1803
qfe4373fc					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QFE4-010621/1804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1805
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1806
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1808
qfe4455fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFE4-010621/1809
qfe4465fc					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QFE4-010621/1810

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-2021-1925**	2021-bulletin	
qfs2530					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1811
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1812
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1815
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1816

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1817
qfs2580					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1818
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1820
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1821
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QFS2-010621/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1823
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1824
qfs2608					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QFS2-010621/1825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1826
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1827
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1829
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1830
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfs2630					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1832
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1833
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1835
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1836
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QFS2-010621/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QFS2-010621/1838
qln1020					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1839
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1841
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QLN1-010621/1843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1844
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1845
qln1021aq					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QLN1-010621/1846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1847
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1848
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1849

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1850
qln1030					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1851
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1853
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1854
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QLN1-010621/1855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1856
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1857
qln1031					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-QLN1-010621/1858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1859
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1860
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1861

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1862
qln1035bd					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QLN1-010621/1863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
qln1036aq					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1864
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1867
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN1-010621/1868
qln4640					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1870
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1871
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1872
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QLN4-010621/1873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1874
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qln4642					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1876
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1877
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1878
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QLN4-010621/1879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1880
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QLN4-010621/1881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1882
qln4650					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1883
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1885
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1886
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1888
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN4-010621/1889
qln5020					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1891
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1892
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1893
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QLN5-010621/1894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1895
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qln5030					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1897
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1898
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1899
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QLN5-010621/1900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1901
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QLN5-010621/1902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1903
qln5040					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1904
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1906
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1907
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1909
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QLN5-010621/1910
qpa2625					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1912
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1913
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1914
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QPA2-010621/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1916
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA2-010621/1917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpa4340					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1918
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1919
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1920
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QPA4-010621/1921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1922
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QPA4-010621/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1924
qpa4360					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1925
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1927
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1930
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1931
qpa4361					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1933
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1934
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1935
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QPA4-010621/1936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1937
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA4-010621/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpa5373					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1939
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1940
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1941
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QPA5-010621/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1943
qpa5460					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1945
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1946
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1948
qpa5461					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1949
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1950
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-QPA5-010621/1951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1953
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-QPA5-010621/1954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1955
qpa5580					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1956
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-QPA5-010621/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1958
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1960

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1961
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qpa5581					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1963
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1964
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1965
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA5-010621/1966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1967
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA5-010621/1968
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QPA5-010621/1969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qpa6560					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA6-010621/1970
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA6-010621/1971
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA6-010621/1972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA6-010621/1973
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA6-010621/1974
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA6-010621/1975

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA6-010621/1976
qpa8673					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1977
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1979
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1980
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPA8-010621/1981

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1982
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1983
qpa8675					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1984
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1985
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1986
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1988
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1989
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QPA8-010621/1990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpa8686					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1991
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1992
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/1993

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1994
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1995
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1996

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1997
qpa8688					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QPA8-010621/1998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
qpa8801					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/1999
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2000
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2001
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-QPA8-010621/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2003
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2005
qpa8802					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2006
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2007
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-QPA8-010621/2008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2009
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2010
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-QPA8-010621/2011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2012
qpa8803					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2013
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-QPA8-010621/2014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2015
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2017

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2018
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qpa8821					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2020
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2021
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2022
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2024
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2025
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-QPA8-010621/2026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qpa8842					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2027
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2028
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/2029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2030
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2031
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPA8-010621/2032

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPA8-010621/2033
qpm2630					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM2-010621/2034
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM2-010621/2035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM2-010621/2036
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM2-010621/2037
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM2-010621/2038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM2-010621/2039
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM2-010621/2040
qpm4621					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2041
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2042
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2043
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM4-010621/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2045
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2046
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QPM4-010621/2047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpm4630					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2048
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2049
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM4-010621/2050

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2051
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2052
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2053

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2054
qpm4640					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2055
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM4-010621/2056

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2057
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM4-010621/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2060
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2061
qpm4641					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QPM4-010621/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2063
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2064
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2066
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2067
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM4-010621/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm4650					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2069
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2070
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2072
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2073
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QPM4-010621/2074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM4-010621/2075
qpm5541					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2076
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2078
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2079
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2080

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2081
qpm5577					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2082
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2085
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2086

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2087
qpm5579					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2088
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2090
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2091
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-QPM5-010621/2092

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2093
qpm5620					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2094
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	H-QUA-QPM5-010621/2095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2096
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2097
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2098

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2099
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2100
qpm5621					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2101
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2102
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2103
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2105
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2106
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QPM5-010621/2107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpm5641					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2108
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2109
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2110

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2111
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2112
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2113

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2114
qpm5657					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2115
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2116

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2117
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2118
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM5-010621/2119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2120
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2121
qpm5658					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QPM5-010621/2122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2123
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2124
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2126
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2127
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM5-010621/2128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm5670					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2129
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2130
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2132
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2133
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QPM5-010621/2134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2135
qpm5677					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2136
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2138
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2139
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM5-010621/2140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2141
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2142
qpm5679					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QPM5-010621/2143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2144
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2145
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2147
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2148
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpm5870					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2150
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2151
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2154
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QPM5-010621/2155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2156
qpm5875					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2157
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2159
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2160
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM5-010621/2161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2162
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM5-010621/2163
qpm6325					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QPM6-010621/2164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2165
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM6-010621/2167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2168
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2169
qpm6375					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QPM6-010621/2170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2171
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2172
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2173

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2174
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2175
qpm6582					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2176
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2177
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2178
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM6-010621/2179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2180
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2181
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-QPM6-010621/2182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpm6585					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2183
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2184
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM6-010621/2185

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2187
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2188

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2189
qpm6621					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2190
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM6-010621/2191

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2192
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2193
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM6-010621/2194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2195
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2196
qpm6670					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QPM6-010621/2197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2198
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2199
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2201
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM6-010621/2202
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-QPM6-010621/2203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm8820					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2204
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2205
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2208
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QPM8-010621/2209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2210
qpm8830					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2211
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2213
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2214
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QPM8-010621/2215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2216
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2217
qpm8870					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QPM8-010621/2218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2219
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2220
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2222
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2223
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpm8895					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2225
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2226
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2229
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QPM8-010621/2230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QPM8-010621/2231
qsm7250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2232
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2234
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QSM7-010621/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2237
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM7-010621/2238
qsm8250					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	H-QUA-QSM8-010621/2239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSM8-010621/2240
qsm8350					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QSM8-010621/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
qsw6310					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2242
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2243
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2244
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-QSW6-010621/2245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2246
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW6-010621/2248
qsw8573					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2249
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2251
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2252
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2254
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2255
qsw8574					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2257
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2258
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2259
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QSW8-010621/2260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2261
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QSW8-010621/2262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qtc410s					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC4-010621/2263
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC4-010621/2264
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC4-010621/2265
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-QTC4-010621/2266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC4-010621/2267
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-QTC4-010621/2268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC4-010621/2269
qtc800h					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2270
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2272
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2273
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2275
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2276
qtc800s					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2278
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2279
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2280
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-QTC8-010621/2281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2282
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qtc800t					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2284
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2285
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QTC8-010621/2286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
qtc801s					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2287
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2288
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2291
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-QTC8-010621/2292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTC8-010621/2293
qtm525					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2294
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2296
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2297
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QTM5-010621/2298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2299
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2300
qtm527					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-QTM5-010621/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2302
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2303
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-QTM5-010621/2304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2305
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QTM5-010621/2306
qualcomm215					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-QUAL-010621/2307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QUAL-010621/2308
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QUAL-010621/2309
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QUAL-010621/2310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-QUAL-010621/2311
rgr7640au					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RGR7-010621/2312
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RGR7-010621/2313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RGR7-010621/2314
rsw8577					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RSW8-010621/2315
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RSW8-010621/2316
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure.	https://www.qualcomm.com/company/product-	H-QUA-RSW8-010621/2317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RSW8-010621/2318
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RSW8-010621/2319
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-RSW8-010621/2320

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-RSW8-010621/2321
sa2150p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA21-010621/2322
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	H-QUA-SA21-010621/2323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA21-010621/2324
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA21-010621/2325
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group	https://www.qualcomm.com/compa	H-QUA-SA21-010621/2326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA21-010621/2327
sa415m					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA41-010621/2328
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-SA41-010621/2329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA41-010621/2330
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-SA41-010621/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA41-010621/2332
sa515m					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA51-010621/2333
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA51-010621/2334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA51-010621/2335
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA51-010621/2336
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SA51-010621/2337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA51-010621/2338
sa6145p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2339
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2341
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2342
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SA61-010621/2343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2344
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2345
sa6150p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SA61-010621/2346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2347
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2348
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2350
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2351
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sa6155					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2353
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2354
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2357
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SA61-010621/2358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2359
sa6155p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2360
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2362
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2363
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SA61-010621/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2365
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA61-010621/2366
sa8150p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SA81-010621/2367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2368
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2369
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2371
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2372
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sa8155					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2374
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2375
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2377
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2378
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SA81-010621/2379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2380
sa8155p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2381
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2383
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2384
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SA81-010621/2385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2386
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2387
sa8195p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SA81-010621/2388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2389
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2390
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2392
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2393
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SA81-010621/2394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sc8180x\\+sdx55					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SC81-010621/2395
sd205					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD20-010621/2396
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD20-010621/2397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD20-010621/2398
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD20-010621/2399
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-SD20-010621/2400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd210					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD21-010621/2401
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD21-010621/2402
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD21-010621/2403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD21-010621/2404
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD21-010621/2405
sd429					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD42-010621/2406
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD42-010621/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD42-010621/2408
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD42-010621/2409
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD42-010621/2410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd439					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD43-010621/2411
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD43-010621/2412
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD43-010621/2413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD43-010621/2414
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD43-010621/2415
sd450					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2416
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-SD45-010621/2417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2418
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2419
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd455					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2421
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2422
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD45-010621/2423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD45-010621/2424
sd460					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2425
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2427
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2428
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD46-010621/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2430
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD46-010621/2431
sd480					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SD48-010621/2432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2433
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2434
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2436
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2437
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD48-010621/2438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd632					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2439
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2440
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2442
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2443
sd636					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2445
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2446
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD63-010621/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD63-010621/2448
sd660					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2449
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2451
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD66-010621/2453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2454
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2455
sd662					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SD66-010621/2456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2457
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2458
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2460
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2461
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd665					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2463
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2464
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2466
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2467
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SD66-010621/2468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD66-010621/2469
sd670					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2470
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2472
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2473
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD67-010621/2474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2475
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2476
sd675					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SD67-010621/2477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2478
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2479
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2481
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2482
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd678					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2484
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2485
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2487
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2488
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SD67-010621/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD67-010621/2490
sd6905g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2491
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2493
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2494
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD69-010621/2495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2496
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD69-010621/2497
sd710					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SD71-010621/2498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2499
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2500
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2502
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2503
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd712					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD71-010621/2505
sd720g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD72-010621/2506
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD72-010621/2507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD72-010621/2508
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD72-010621/2509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD72-010621/2510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD72-010621/2511
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD72-010621/2512
sd730					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD73-010621/2513
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD73-010621/2514
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD73-010621/2515
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD73-010621/2516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD73-010621/2517
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD73-010621/2518
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-SD73-010621/2519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
sd750g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2520
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2521
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD75-010621/2522

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2524
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2525

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD75-010621/2526
sd765					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2527
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD76-010621/2528

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2529
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD76-010621/2531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2532
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2533
sd765g					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-SD76-010621/2534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2535
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2536
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2538
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2539
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD76-010621/2540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
sd768g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2541
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2542
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2544
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2545
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SD76-010621/2546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD76-010621/2547
sd7c					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD7C-010621/2548
sd835					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD83-010621/2549
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD83-010621/2550
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD83-010621/2551
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-SD83-010621/2552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD83-010621/2553
sd845					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD84-010621/2554
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of	https://www.qualcomm.com/compa	H-QUA-SD84-010621/2555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	ny/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD84-010621/2556
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD84-010621/2557
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SD84-010621/2558

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD84-010621/2559
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD84-010621/2560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
sd850					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2561
sd855					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2562
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2564
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2565
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2567
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD85-010621/2568
sd8655g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2570
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2571
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2572
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-SD86-010621/2573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2574
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD86-010621/2575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd870					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD87-010621/2576
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD87-010621/2577
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD87-010621/2578
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-SD87-010621/2579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD87-010621/2580
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-SD87-010621/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD87-010621/2582
sd888					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2583
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2585
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2588
sd8885g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2589
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2590
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-SD88-010621/2591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2592
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2593
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-SD88-010621/2594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD88-010621/2595
sd8c					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2596
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-SD8C-010621/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2599
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper	https://www.qualcomm	H-QUA-SD8C-010621/2600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2601
sd8cx					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2603
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SD8C-010621/2605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2606
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SD8C-010621/2607
sda429w					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SDA4-010621/2608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDA4-010621/2609
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDA4-010621/2610
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDA4-010621/2611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDA4-010621/2612
sdm429w					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM4-010621/2613
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM4-010621/2614
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-SDM4-010621/2615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM4-010621/2616
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM4-010621/2617
sdm630					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-SDM6-010621/2618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM6-010621/2619
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM6-010621/2620
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM6-010621/2621

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM6-010621/2622
sdm830					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM8-010621/2623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM8-010621/2624
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM8-010621/2625
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM8-010621/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDM8-010621/2627
sdr051					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2628
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2629
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-SDR0-010621/2630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2631
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2632
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-SDR0-010621/2633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2634
sdr052					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2635
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-SDR0-010621/2636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2637
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2638
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2639

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2640
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR0-010621/2641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdr425					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR4-010621/2642
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR4-010621/2643
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR4-010621/2644
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR4-010621/2645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR4-010621/2646
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR4-010621/2647
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-SDR4-010621/2648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
sdr660					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2649
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2650
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR6-010621/2651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2652
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2653
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR6-010621/2654

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2655
sdr660g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2656
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR6-010621/2657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2658
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2659
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SDR6-010621/2660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2661
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2662
sdr675					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2663
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2664
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2665
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR6-010621/2666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2667
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR6-010621/2668
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-SDR6-010621/2669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
sdr735					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2670
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2671
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR7-010621/2672

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2673
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2674
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2675

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2676
sdr735g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2677
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR7-010621/2678

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2679
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2680
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SDR7-010621/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2682
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR7-010621/2683
sdr8150					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	H-QUA-SDR8-010621/2684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2685
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2686
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2688
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2689
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDR8-010621/2690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
sdr8250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2691
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2692
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2694
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2695
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SDR8-010621/2696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2697
sdr845					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2698
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2700
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2701
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-SDR8-010621/2702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sdr865					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2703
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2704
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2706
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2707
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-SDR8-010621/2708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDR8-010621/2709
sdw2500					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDW2-010621/2710
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDW2-010621/2711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
sdw3100					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDW3-010621/2712
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDW3-010621/2713
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDW3-010621/2714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDW3-010621/2715
sdx20					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2716
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2718
sdx20m					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2719
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2721
sdx24					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2722
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2723
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SDX2-010621/2724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX2-010621/2725
sdx50m					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2726
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2728
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SDX5-010621/2730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2731
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2732
sdx55					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SDX5-010621/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2734
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2735
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2737
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2738
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sdx55m					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2740
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2741
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2743
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2744
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SDX5-010621/2745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDX5-010621/2746
sdxr1					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2747
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2749
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2750
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SDXR-010621/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2752
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2753
sdxr25g					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SDXR-010621/2754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2755
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2756
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SDXR-010621/2757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2758
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SDXR-010621/2759
sdxr2_5g					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	H-QUA-SDXR-010621/2760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
sm4125					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2761
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2762
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2764
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2765
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SM41-010621/2766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM41-010621/2767
sm6250					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2768
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2770
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2771
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SM62-010621/2772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2773
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2774
sm6250p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-SM62-010621/2775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2776
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2777
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2779
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2780
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM62-010621/2781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sm7250p					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2782
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2783
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2785
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2786
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-SM72-010621/2787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM72-010621/2788
sm7350					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM73-010621/2789
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM73-010621/2790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM73-010621/2791
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SM73-010621/2792
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	H-QUA-SM73-010621/2793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1350					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2794
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2795
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**		
smb1351					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2797
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2798
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2799
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-SMB1-010621/2800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2801
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-SMB1-010621/2802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2803
smb1354					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2804
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2806
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2807
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2809
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2810
smb1355					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2812
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2813
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2814
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-SMB1-010621/2815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2816
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1357					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2818
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2819
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
smb1358					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2821
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2822
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2823
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-SMB1-010621/2824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2825
smb1360					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2826
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2828
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2829
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1380					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2831
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2832
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2833
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	H-QUA-SMB1-010621/2834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2835
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-SMB1-010621/2836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2837
smb1381					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2838
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2840
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2841
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2843
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2844
smb1390					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2846
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2847
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2848
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-SMB1-010621/2849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2850
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1394					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2852
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2853
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2854
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	H-QUA-SMB1-010621/2855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2856
smb1395					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2857
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	H-QUA-SMB1-010621/2858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2859
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2860
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2861

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2862
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2863
smb1396					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2864
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2865
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2866
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMB1-010621/2867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2868
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2869
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-SMB1-010621/2870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
smb1398					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2871
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2872
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMB1-010621/2873

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2874
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2875
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2876

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB1-010621/2877
smb231					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2879
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2880
smb2351					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2881
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2884
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMB2-010621/2885

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB2-010621/2886
smb358s					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB3-010621/2887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMB3-010621/2888
smr525					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2889
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2890
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMR5-010621/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2893
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMR5-010621/2894

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2895
smr526					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2896
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMR5-010621/2897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2898
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2899
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-SMR5-010621/2900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2901
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2902
smr545					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2903
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2904
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2905
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMR5-010621/2906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2907
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2908
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-SMR5-010621/2909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
smr546					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2910
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2911
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-SMR5-010621/2912

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2913
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2914
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2915

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-SMR5-010621/2916
wcd9326					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2917
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCD9-010621/2918

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2919
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCD9-010621/2921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2922
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2923
wcd9330					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2924
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2925
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2926
wcd9335					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2927
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2928
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2929
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCD9-010621/2930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2931
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2932
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-WCD9-010621/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wcd9340					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2934
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2935
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCD9-010621/2936

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2938
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2939

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2940
wcd9341					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2941
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCD9-010621/2942

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2943
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCD9-010621/2945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2946
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2947
wcd9360					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2948
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2949
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCD9-010621/2951

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2952
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wcd9370					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2954
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2955
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2956
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WCD9-010621/2957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2958
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2960
wcd9371					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2961
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2963
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2964
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2966
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2967
wcd9375					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2969
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2970
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2971
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	H-QUA-WCD9-010621/2972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2973
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcd9380					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2975
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2976
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2978
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2979
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-WCD9-010621/2980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2981
wcd9385					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2982
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2984
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2985
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2987
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCD9-010621/2988
wcn3610					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2989

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2990
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2991
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2992
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-WCN3-010621/2993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wcn3615					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2994
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2995
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCN3-010621/2996

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2997
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/2998
wcn3620					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCN3-010621/2999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3000
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3001
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3003
wcn3660					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3004
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3006
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3007
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3008
wcn3660b					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3009
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3010
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3011
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCN3-010621/3012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3013
wcn3680					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3014
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3016
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3017
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wcn3680b					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3019
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3020
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3021
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WCN3-010621/3022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3023
wcn3910					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3024
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3026
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCN3-010621/3028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3029
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3030
wcn3950					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-WCN3-010621/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3032
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3033
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3035
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3036
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn3980					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3038
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3039
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3042
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-WCN3-010621/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3044
wcn3988					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3045
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3047
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCN3-010621/3049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3050
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3051
wcn3990					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-WCN3-010621/3052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3053
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3054
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3056
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3057
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn3991					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3059
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3060
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3062
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3063
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-WCN3-010621/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3065
wcn3998					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3066
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3068
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3069
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCN3-010621/3070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3071
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3072
wcn3999					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	H-QUA-WCN3-010621/3073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3074
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3075
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3077
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3078
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN3-010621/3079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn6740					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3080
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3081
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3083
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3084
wcn6745					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3085

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-2021-1925**		
wcn6750					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3086
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3087
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCN6-010621/3088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
wcn6850					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3089
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3090
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3092
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3093
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	H-QUA-WCN6-010621/3094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3095
wcn6851					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3096
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3098
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3101
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3102
wcn6855					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3103

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-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3104
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3105
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	H-QUA-WCN6-010621/3106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3107
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3108
wcn6856					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3109
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3110
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3111
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WCN6-010621/3112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3113
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WCN6-010621/3114
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	H-QUA-WCN6-010621/3115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wgr7640					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3116
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3117
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WGR7-010621/3118

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3120
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3121

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WGR7-010621/3122
whs9410					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	H-QUA-WHS9-010621/3123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
wsa8810					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3124
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3125
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3126
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WSA8-010621/3127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3128
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3130
wsa8815					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3131
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3132
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	H-QUA-WSA8-010621/3133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3134
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3135
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	H-QUA-WSA8-010621/3136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3137
wsa8830					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3138
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	H-QUA-WSA8-010621/3139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3140
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3141
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3142

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3143
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8835					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3145
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3146
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3147
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WSA8-010621/3148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3149
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WSA8-010621/3150
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	H-QUA-WSA8-010621/3151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
wtr2955					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3152
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3153
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WTR2-010621/3154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3155
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3156
wtr2965					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-	H-QUA-WTR2-010621/3157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3158
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3159
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3161
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3162
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR2-010621/3163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wtr3925					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3164
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3165
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3167
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3168
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	H-QUA-WTR3-010621/3169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR3-010621/3170
wtr4905					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR4-010621/3171
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR4-010621/3172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR4-010621/3173
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR4-010621/3174
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR4-010621/3175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wtr5975					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3176
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3177
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3178
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-WTR5-010621/3179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3180
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR5-010621/3182
wtr6955					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3183
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3185
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3188
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	H-QUA-WTR6-010621/3189
Tenda					
ac11					
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setmac allows	N/A	H-TEN-AC11-010621/3190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to execute arbitrary code on the system via a crafted post request. **CVE ID : CVE-2021-31755**		
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setwanType allows attackers to execute arbitrary code on the system via a crafted post request. This occurs when input vector controlled by malicious attack get copied to the stack variable. **CVE ID : CVE-2021-31756**	N/A	H-TEN-AC11-010621/3191
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setVLAN allows attackers to execute arbitrary code on the system via a crafted post request. **CVE ID : CVE-2021-31757**	N/A	H-TEN-AC11-010621/3192
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setportList allows attackers to execute arbitrary code on the	N/A	H-TEN-AC11-010621/3193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system via a crafted post request. **CVE ID : CVE-2021-31758**		
Operating System					
Amazon					
freertos					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-05-2021	7.5	The kernel in Amazon Web Services FreeRTOS before 10.4.3 has insufficient bounds checking during management of heap memory. **CVE ID : CVE-2021-32020**	https://github.com/FreeRTOS/FreeRTOS-Kernel/commit/c7a9a01c94987082b223d3e59969ede64363da63	O-AMA-FREE-010621/3194
Asus					
gt-ac2900_firmware					
Improper Authentication	06-05-2021	7.5	The administrator application on ASUS GT-AC2900 devices before 3.0.0.4.386.42643 allows authentication bypass when processing remote input from an unauthenticated user, leading to unauthorized access to the administrator interface. This relates to handle_request in router/httpd/httpd.c and auth_check in web_hook.o. An attacker-supplied value of '\0' matches the device's default value of '\0' in some situations. **CVE ID : CVE-2021-32030**	https://www.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-Gaming-Routers/RT-AC2900/HelpDesk_BIOS/	O-ASU-GT-A-010621/3195
Cisco					
asyncos					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Sensitive Information in Source Code	06-05-2021	4	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA), Cisco Email Security Appliance (ESA), and Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface. **CVE ID : CVE-2021-1516**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-sma-info-gY2AEz2H	O-CIS-ASYN-010621/3196
c125_m5_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C125-010621/3197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c220_m5_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C220-010621/3198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c220_m6_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C220-010621/3199
c225_m6_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C225-010621/3200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c240_m5_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C240-010621/3201
c240_m6_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C240-010621/3202
c245_m6_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C245-010621/3203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
c480_m5_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C480-010621/3204
c480_ml_m5_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-C480-010621/3205
encs_5100_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-ENCS-010621/3206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
encs_5400_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-ENCS-010621/3207
hyperflex_hx_data_platform					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	10	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1497**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR	O-CIS-HYPE-010621/3208
roomos					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-05-2021	4	A vulnerability in the video endpoint API (xAPI) of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an authenticated, remote attacker to read arbitrary files from the underlying operating system. This vulnerability is due to insufficient path validation of command arguments. An attacker could exploit this vulnerability by sending a crafted command request to the xAPI. A successful exploit could allow the attacker to read the contents of any file that is located on the device filesystem. **CVE ID : CVE-2021-1532**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tp-rmos-fileread-pE9sL3g	O-CIS-ROOM-010621/3209
rv340w_firmware					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340,	https://tools.cisco.com/security/cen	O-CIS-RV34-010621/3210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**	ter/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	
rv340_firmware					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	O-CIS-RV34-010621/3211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**		
rv345p_firmware					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	O-CIS-RV34-010621/3212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**		
rv345_firmware					
Write-what-where Condition	06-05-2021	7.2	A vulnerability in the internal message processing of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an authenticated, local attacker to run arbitrary commands with root privileges on the underlying operating system (OS). This vulnerability exists because an internal messaging service does not properly sanitize input. An attacker could exploit this vulnerability by first authenticating to the device and then sending a crafted request to the internal service. A successful exploit could allow the attacker to run arbitrary commands with root privileges on the underlying OS. To exploit this vulnerability, the attacker must have valid Administrator credentials for the device. **CVE ID : CVE-2021-1520**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-34x-privesc-GLN8ZAQE	O-CIS-RV34-010621/3213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ucs_e1120d_m3_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3214
ucs_e140dp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e140d_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3216
ucs_e140s_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3217
ucs_e140s_m1_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e140s_m2_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3219
ucs_e160dp_m1_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3220
ucs_e160d_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_e160s_m3_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3222
ucs_e180d_m2_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3223
ucs_e180d_m3_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**		
ucs_s3260_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	06-05-2021	5.8	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. This vulnerability is known as an open redirect attack, which is used in phishing attacks to get users to visit malicious sites without their knowledge. **CVE ID : CVE-2021-1397**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imc-openred-zAYrU6d2	O-CIS-UCS_-010621/3225
vedge-100b_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3226
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3227
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3228
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3230
vedge-cloud_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3231
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3232
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3233
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3235
vedge_1000_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3236
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3237
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3238
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3240
vedge_100b_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3241
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3242
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3243
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3245
vedge_100m_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3246
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3247
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3248
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3250
vedge_100wm_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3251
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3252
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3253
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3255
vedge_100_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3256
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3257
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3258
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3260
vedge_2000_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3261
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3262
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3263
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3265
vedge_5000_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	8.5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1509**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3266
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	5	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1510**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3267
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-05-2021	6.8	Multiple vulnerabilities in Cisco SD-WAN vEdge Software could allow an attacker to execute arbitrary code as the root user or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1511**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-buffover-MWGucjtO	O-CIS-VEDG-010621/3268
Files or Directories Accessible	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an	https://tools.cisco.com/security/cen	O-CIS-VEDG-010621/3269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to External Parties			authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	ter/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VEDG-010621/3270
vsmart_controller_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Files or Directories Accessible to External Parties	06-05-2021	3.6	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to overwrite arbitrary files in the underlying file system of an affected system. This vulnerability is due to insufficient validation of the user-supplied input parameters of a specific CLI command. An attacker could exploit this vulnerability by issuing that command with specific parameters. A successful exploit could allow the attacker to overwrite the content in any arbitrary files that reside on the underlying host file system. **CVE ID : CVE-2021-1512**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfile-7Qhd9mCn	O-CIS-VSMA-010621/3271
Improper Input Validation	06-05-2021	7.8	A vulnerability in the vDaemon process of Cisco SD-WAN Software could allow an unauthenticated, remote attacker to cause a device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2021-1513**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dos-Ckn5cVqW	O-CIS-VSMA-010621/3272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Debian					
debian_linux					
Unrestricted Upload of File with Dangerous Type	05-05-2021	5	In Django 2.2 before 2.2.21, 3.1 before 3.1.9, and 3.2 before 3.2.1, MultiPartParser, UploadedFile, and FieldFile allowed directory traversal via uploaded files with suitably crafted file names. **CVE ID : CVE-2021-31542**	https://www.djangoproject.com/weblog/2021/may/04/security-releases/, https://docs.djangoproject.com/en/3.2/releases/security/, http://www.openwall.com/lists/oss-security/2021/05/04/3	O-DEB-DEBI-010621/3273
Dell					
emc_powerscale_onefs					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	7.2	Dell PowerScale OneFS 8.1.0-9.1.0 contain an improper neutralization of special elements used in an OS command vulnerability. This vulnerability may allow an authenticated user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges to escalate privileges. **CVE ID : CVE-2021-21527**	https://www.dell.com/support/kbdoc/000185978	O-DEL-EMC_-010621/3274
Improper Neutralization of Special Elements used in an OS Command ('OS	06-05-2021	7.2	Dell EMC PowerScale OneFS 8.1.0-9.1.0 contain an improper neutralization of special elements used in an OS command vulnerability. This vulnerability can allow an authenticated user with	https://www.dell.com/support/kbdoc/000185978	O-DEL-EMC_-010621/3275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE privileges to escalate privileges. **CVE ID : CVE-2021-21550**		
Fedoraproject					
fedora					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**	https://bugzilla.suse.com/show_bug.cgi?id=1184161	O-FED-FEDO-010621/3276
Unrestricted Upload of File with Dangerous Type	05-05-2021	5	In Django 2.2 before 2.2.21, 3.1 before 3.1.9, and 3.2 before 3.2.1, MultiPartParser, UploadedFile, and FieldFile allowed directory traversal	https://www.djangoproject.com/weblog/2021/may/04/security-	O-FED-FEDO-010621/3277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via uploaded files with suitably crafted file names. **CVE ID : CVE-2021-31542**	releases/, https://docs.djangoproject.com/en/3.2/releases/security/, http://www.openwall.com/lists/oss-security/2021/05/04/3	
Incorrect Authorization	06-05-2021	2.1	kernel/bpf/verifier.c in the Linux kernel through 5.12.1 performs undesirable speculative loads, leading to disclosure of stack content via side-channel attacks, aka CID-801c6058d14a. The specific concern is not protecting the BPF stack area against speculative loads. Also, the BPF stack can contain uninitialized data that might represent sensitive information previously operated on by the kernel. **CVE ID : CVE-2021-31829**	http://www.openwall.com/lists/oss-security/2021/05/04/4, https://github.com/torvalds/linux/commit/801c6058d14a82179a7ee17a4b532cac6fad067f	O-FED-FEDO-010621/3278
Out-of-bounds Read	05-05-2021	5.5	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into	https://www.samba.org/samba/security/CVE-2021-20254.html	O-FED-FEDO-010621/3279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity. **CVE ID : CVE-2021-20254**		
hongdian					
h8922_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-05-2021	4	Hongdian H8922 3.0.5 devices allow Directory Traversal. The /log_download.cgi log export handler does not validate user input and allows a remote attacker with minimal privileges to download any file from the device by substituting ../ (e.g., ../../etc/passwd) This can be carried out with a web browser by changing the file name accordingly. Upon visiting log_download.cgi?type=../../etc/passwd and logging in, the web server will allow a download of the contents of the /etc/passwd file. **CVE ID : CVE-2021-28149**	http://en.hongdian.com/Products/Details/H8922	O-HON-H892-010621/3280
Improper Input Validation	06-05-2021	2.1	Hongdian H8922 3.0.5 devices allow the unprivileged guest user to read cli.conf (with the administrator password and other sensitive data) via /backup2.cgi. **CVE ID : CVE-2021-28150**	http://en.hongdian.com/Products/Details/H8922	O-HON-H892-010621/3281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-05-2021	9	Hongdian H8922 3.0.5 devices allow OS command injection via shell metacharacters into the ip-address (aka Destination) field to the tools.cgi ping command, which is accessible with the username guest and password guest. **CVE ID : CVE-2021-28151**	http://en.hongdian.com/Products/Details/H8922	O-HON-H892-010621/3282
Use of Hard-coded Credentials	06-05-2021	7.5	Hongdian H8922 3.0.5 devices have an undocumented feature that allows access to a shell as a superuser. To connect, the telnet service is used on port 5188 with the default credentials of root:superzxmn. **CVE ID : CVE-2021-28152**	http://en.hongdian.com/Products/Details/H8922	O-HON-H892-010621/3283
Linux					
linux_kernel					
Incorrect Authorization	06-05-2021	2.1	kernel/bpf/verifier.c in the Linux kernel through 5.12.1 performs undesirable speculative loads, leading to disclosure of stack content via side-channel attacks, aka CID-801c6058d14a. The specific concern is not protecting the BPF stack area against speculative loads. Also, the BPF stack can contain uninitialized data that might represent sensitive information previously operated on by the kernel. **CVE ID : CVE-2021-31829**	http://www.openwall.com/lists/oss-security/2021/05/04/4, https://github.com/torvalds/linux/commit/801c6058d14a82179a7ee17a4b532cac6fad067f	O-LIN-LINU-010621/3284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	10-05-2021	4.4	net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller. **CVE ID : CVE-2021-32399**	https://github.com/torvalds/linux/commit/e2cb6b891ad2b8caa9131e3be70f45243df82a80, https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=e2cb6b891ad2b8caa9131e3be70f45243df82a80, http://www.openwall.com/lists/oss-security/2021/05/11/2	O-LIN-LINU-010621/3285
Out-of-bounds Write	06-05-2021	3.6	A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an array index, which can be updated by a user process at anytime which could lead to an out-of-bounds write. The highest threat from this vulnerability is to data integrity and system availability. **CVE ID : CVE-2021-3501**	https://bugzilla.redhat.com/show_bug.cgi?id=1950136, https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=04c4f2ee3f68c9a4bf1653d15f1a9a435ae33f7a	O-LIN-LINU-010621/3286
Microsoft					
windows					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13101. **CVE ID : CVE-2021-31441**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3287
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. Was ZDI-CAN-13239. **CVE ID : CVE-2021-31442**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13240. **CVE ID : CVE-2021-31443**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3289
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13241. **CVE ID : CVE-2021-31444**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13244. **CVE ID : CVE-2021-31445**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13245. **CVE ID : CVE-2021-31446**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3292
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13269. **CVE ID : CVE-2021-31447**		
Out-of-bounds Read	07-05-2021	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13273. **CVE ID : CVE-2021-31448**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3294
Double Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User	https://www.foxitsoftware.com/support/security-	O-MIC-WIND-010621/3295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in PDF files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13280. **CVE ID : CVE-2021-31449**	bulletins.php	
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13084. **CVE ID : CVE-2021-31450**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13089. **CVE ID : CVE-2021-31451**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3297
Out-of-bounds Write	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			context of the current process. Was ZDI-CAN-13091. **CVE ID : CVE-2021-31452**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13092. **CVE ID : CVE-2021-31453**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3299
Heap-based Buffer Overflow	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Decimal element. A crafted leadDigits value in a Decimal element can trigger an overflow of a	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fixed-length heap-based buffer. An attacker can leverage this vulnerability to execute arbitrary code in the context of the current process. Was ZDI-CAN-13095. **CVE ID : CVE-2021-31454**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13100. **CVE ID : CVE-2021-31455**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3301
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13102. **CVE ID : CVE-2021-31456**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13147. **CVE ID : CVE-2021-31457**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3303
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious file. The specific flaw exists within the handling of Annotation objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13150. **CVE ID : CVE-2021-31458**		
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA Forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13162. **CVE ID : CVE-2021-31459**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3305
Use After Free	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to	https://www.foxitsoftware.com/support/security-	O-MIC-WIND-010621/3306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13096. **CVE ID : CVE-2021-31460**	bulletins.php	
Access of Resource Using Incompatible Type ('Type Confusion')	07-05-2021	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 10.1.1.37576. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the the handling of app.media objects. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process Was ZDI-CAN-13333. **CVE ID : CVE-2021-31461**	https://www.foxitsoftware.com/support/security-bulletins.php	O-MIC-WIND-010621/3307
windows_10					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3308
Exposure of Sensitive Information to an Unauthorized Actor	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479	O-MIC-WIND-010621/3309
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31167, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31165**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31165	O-MIC-WIND-010621/3310
N/A	11-05-2021	7.5	HTTP Protocol Stack Remote Code Execution Vulnerability **CVE ID : CVE-2021-31166**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166	O-MIC-WIND-010621/3311
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31167**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31167	O-MIC-WIND-010621/3312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31168**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31168	O-MIC-WIND-010621/3313
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31168, CVE-2021-31208. **CVE ID : CVE-2021-31169**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31169	O-MIC-WIND-010621/3314
Improper Privilege Management	11-05-2021	4.6	Windows Graphics Component Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31188. **CVE ID : CVE-2021-31170**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31170	O-MIC-WIND-010621/3315
windows_7					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3316
windows_8.1					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-010621/3317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				visory/CVE-2021-28476	
Exposure of Sensitive Information to an Unauthorized Actor	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479	O-MIC-WIND-010621/3318
windows_rt_8.1					
Exposure of Sensitive Information to an Unauthorized Actor	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479	O-MIC-WIND-010621/3319
windows_server_2008					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3320
windows_server_2012					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3321
Exposure of Sensitive Information to an	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-	O-MIC-WIND-010621/3322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor				US/security-guidance/advisory/CVE-2021-28479	
windows_server_2016					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3323
Exposure of Sensitive Information to an Unauthorized Actor	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479	O-MIC-WIND-010621/3324
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31167, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31165**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31165	O-MIC-WIND-010621/3325
N/A	11-05-2021	7.5	HTTP Protocol Stack Remote Code Execution Vulnerability **CVE ID : CVE-2021-31166**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166	O-MIC-WIND-010621/3326
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010621/3327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2021-31168, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31167**	guidance/advisory/CVE-2021-31167	
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31168**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31168	O-MIC-WIND-010621/3328
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31167, CVE-2021-31168, CVE-2021-31208. **CVE ID : CVE-2021-31169**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31169	O-MIC-WIND-010621/3329
Improper Privilege Management	11-05-2021	4.6	Windows Graphics Component Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31188. **CVE ID : CVE-2021-31170**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31170	O-MIC-WIND-010621/3330
windows_server_2019					
N/A	11-05-2021	6.5	Hyper-V Remote Code Execution Vulnerability **CVE ID : CVE-2021-28476**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476	O-MIC-WIND-010621/3331
Exposure of Sensitive Information to an	11-05-2021	2.1	Windows CSC Service Information Disclosure Vulnerability **CVE ID : CVE-2021-28479**	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010621/3332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unauthorized Actor				guidance/advisory/CVE-2021-28479	
Improper Privilege Management	11-05-2021	4.6	Windows Container Manager Service Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31165, CVE-2021-31168, CVE-2021-31169, CVE-2021-31208. **CVE ID : CVE-2021-31167**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31167	O-MIC-WIND-010621/3333
Improper Privilege Management	11-05-2021	4.6	Windows Graphics Component Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-31188. **CVE ID : CVE-2021-31170**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31170	O-MIC-WIND-010621/3334
Opensuse					
leap					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud	https://bugzilla.suse.com/show_bug.cgi?id=1184161	O-OPE-LEAP-010621/3335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**		
Qualcomm					
apq8009w_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3336
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3337
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3339
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3340
apq8009_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3342
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3343
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
apq8017_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3345
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3346
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3347
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-APQ8-010621/3348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3349
apq8053_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3350
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-APQ8-010621/3351

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3352
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3353
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
apq8064au_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3355
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3356
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**		
apq8096au_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3358
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3359
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-APQ8-010621/3361
aqt1000_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3362
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3364
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3365
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3367
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AQT1-010621/3368
ar8031_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3370
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3371
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3372
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-AR80-010621/3373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3374
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ar8035_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3376
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3377
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3378
Buffer Copy without	07-05-2021	7.2	Buffer overflow can occur due to improper validation	https://www.qualcomm	O-QUA-AR80-010621/3379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	.com/company/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR80-010621/3380
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-AR80-010621/3381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ar8151_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR81-010621/3382
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR81-010621/3383
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR81-010621/3384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR81-010621/3385
ar9380_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR93-010621/3386
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-AR93-010621/3387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR93-010621/3388
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-AR93-010621/3389
csr8811_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-CSR8-010621/3390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSR8-010621/3391
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSR8-010621/3392
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-CSR8-010621/3393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
csra6620_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3394
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3395
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-CSRA-010621/3396

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3397
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3398
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3399

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3400
csra6640_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3401
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-CSRA-010621/3402

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3403
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3404
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-CSRA-010621/3405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3406
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRA-010621/3407
csrb31024_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-CSRB-010621/3408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRB-010621/3409
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRB-010621/3410
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-CSRB-010621/3411

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-CSRB-010621/3412
fsm10055_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3414
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3417
fsm10056_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3418
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3420
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-FSM1-010621/3421
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-FSM1-010621/3422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq4018_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3424
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-IPQ4-010621/3425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3426
ipq4019_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3428
ipq4028_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3429
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3431
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3432
ipq4029_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3434
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3435
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ4-010621/3436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq5010_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3437
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3439
ipq5018_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3440
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3441

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ5-010621/3442
ipq6000_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3443
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-IPQ6-010621/3444

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3445
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq6005_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3447
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3448
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-IPQ6-010621/3449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
ipq6010_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3450
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3451
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-IPQ6-010621/3452

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3453
ipq6018_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3454
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-IPQ6-010621/3455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3456
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
ipq6028_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3458
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3459
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-IPQ6-010621/3460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ6-010621/3461
ipq8064_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3462
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-IPQ8-010621/3463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3464
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3465
ipq8065_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-IPQ8-010621/3466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3467
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3468
ipq8068_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-IPQ8-010621/3469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3470
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3471
ipq8069_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-IPQ8-010621/3472

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-2021-1925**	letins/may-2021-bulletin	
ipq8070a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3473
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3474
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3476
ipq8070_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3477
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3479
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8071a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3481
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3482
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-IPQ8-010621/3483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3484
ipq8071_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3485
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-IPQ8-010621/3486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3487
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3488
ipq8072a_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3490
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3491
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
ipq8072_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3493
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3494
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3496
ipq8074a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3497
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3499
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
ipq8074_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3501
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3502
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-IPQ8-010621/3503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3504
ipq8076a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3505
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-IPQ8-010621/3506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3507
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3508
ipq8076_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3510
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3511
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
ipq8078a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3513
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3514
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-010621/3515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3516
ipq8078_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-IPQ8-010621/3517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3518
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3519
ipq8173_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-IPQ8-010621/3520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3521
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3522
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-IPQ8-010621/3523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
ipq8174_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3525
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group	https://www.qualcomm.com/compa	O-QUA-IPQ8-010621/3526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-IPQ8-010621/3527
mdm9150_firmware					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
mdm9206_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3529
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3530
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
mdm9250_firmware					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3532
mdm9607_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3533
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
mdm9626_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3535
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3536
mdm9628_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3538
mdm9650_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3539
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MDM9-010621/3541
msm8909w_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3542
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3543
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-MSM8-010621/3544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3545
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3546
msm8917_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-MSM8-010621/3547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3548
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3549
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3551
msm8953_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3552
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3554
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3555
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3556
msm8996au_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3557
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3558
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-MSM8-010621/3559
pm215_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-PM21-010621/3560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM21-010621/3561
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM21-010621/3562
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM21-010621/3563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM21-010621/3564
pm3003a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3565
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3567
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3568
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3570
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM30-010621/3571
pm4125_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3573
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3574
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3575
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PM41-010621/3576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3577
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM41-010621/3578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm4250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM42-010621/3579
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM42-010621/3580
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM42-010621/3581
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PM42-010621/3582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM42-010621/3583
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM42-010621/3584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pm439_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM43-010621/3585
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM43-010621/3586
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM43-010621/3587
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PM43-010621/3588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM43-010621/3589
pm456_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3590
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3592
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3593
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM45-010621/3594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3595
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM45-010621/3596
pm6125_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM61-010621/3597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3598
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3599
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3601
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3602
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm6150a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3604
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3605
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3608
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM61-010621/3609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3610
pm6150l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3611
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3613
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM61-010621/3615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3616
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3617
pm6150_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM61-010621/3618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3619
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3620
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3622
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3623
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM61-010621/3624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm6250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3625
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3626
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3629
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM62-010621/3630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM62-010621/3631
pm6350_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3632
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3634
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM63-010621/3636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3637
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM63-010621/3638
pm640a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM64-010621/3639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3640
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3641
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3643
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3644
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm640l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3646
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3647
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3650
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM64-010621/3651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3652
pm640p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3653
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3655
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM64-010621/3657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3658
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM64-010621/3659
pm660a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM66-010621/3660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3661
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3662
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3664
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3665
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm660l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3667
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3668
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3671
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM66-010621/3672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3673
pm660_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3674
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3676
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3677
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM66-010621/3678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3679
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM66-010621/3680
pm670a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM67-010621/3681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3682
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3683
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3685
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3686
pm670l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3688
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3689
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3690
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-PM67-010621/3691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3692
pm670_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3693
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-PM67-010621/3694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3695
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3696
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3697

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM67-010621/3698
pm7150a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3699
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PM71-010621/3700

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3701
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3702
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM71-010621/3703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3704
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3705
pm7150l_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-PM71-010621/3706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3707
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3708
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3710
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM71-010621/3711
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PM71-010621/3712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pm7250b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3713
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3714
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3716
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3717
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM72-010621/3718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3719
pm7250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3720
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3722
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM72-010621/3724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3725
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM72-010621/3726
pm7350c_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM73-010621/3727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM73-010621/3728
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM73-010621/3729
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM73-010621/3730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM73-010621/3731
pm8004_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3732
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3734
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3735
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3737
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3738
pm8005_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3740
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3741
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3742
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PM80-010621/3743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3744
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8008_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3746
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3747
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3748
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PM80-010621/3749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3750
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-PM80-010621/3751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3752
pm8009_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3753
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3755
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3756
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3758
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM80-010621/3759
pm8150a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3761
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3762
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3763
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PM81-010621/3764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3765
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8150b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3767
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3768
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3769
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PM81-010621/3770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3771
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-PM81-010621/3772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3773
pm8150c_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3774
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3776
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3777
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3779
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3780
pm8150l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3782
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3783
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3784
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PM81-010621/3785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3786
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8150_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3788
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3789
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3790
Buffer Copy without	07-05-2021	7.2	Buffer overflow can occur due to improper validation	https://www.qualcomm	O-QUA-PM81-010621/3791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	.com/company/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM81-010621/3792
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-PM81-010621/3793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3794
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3795
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3796

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3798
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-PM82-010621/3799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM82-010621/3800
pm8350bhs_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3801
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3803
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3804
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8350bh_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3806
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3807
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3808
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PM83-010621/3809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3810
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-PM83-010621/3811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3812
pm8350b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3813
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3815
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3816
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3818
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3819
pm8350c_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3821
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3822
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3823
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PM83-010621/3824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3825
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8350_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3827
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3828
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3829
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PM83-010621/3830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3831
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-PM83-010621/3832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM83-010621/3833
pm855a_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3834
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3836
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3837
pm855b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM85-010621/3838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3839
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3840
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3842
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3843
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm855l_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3845
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3846
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3848
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3849
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PM85-010621/3850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3851
pm855p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3852
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3854
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3855
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PM85-010621/3856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3857
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3858
pm855_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PM85-010621/3859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3860
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3861
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3863
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3864
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM85-010621/3865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pm8909_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3866
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3867
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3869
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3870
pm8916_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3871
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of	https://www.qualcomm	O-QUA-PM89-010621/3872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	.com/company/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3873
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3874
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PM89-010621/3875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
pm8937_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3876
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3877
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3879
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3880
pm8953_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3882
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3883
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3884
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-PM89-010621/3885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
pm8998_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3886
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3887
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PM89-010621/3888

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3890
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3891

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PM89-010621/3892
pmc1000h_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMC1-010621/3893
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMC1-010621/3894

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMC1-010621/3895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMC1-010621/3896
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMC1-010621/3897

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMC1-010621/3898
pmc7180_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-PMC7-010621/3899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
pmd9607_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3900
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3901
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3902

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
pmd9655au_firmware					
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3903
pmd9655_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3904
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3905
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-PMD9-010621/3906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3907
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3908
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-PMD9-010621/3909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMD9-010621/3910
pme605_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PME6-010621/3911
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-PME6-010621/3912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PME6-010621/3913
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PME6-010621/3914
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PME6-010621/3915

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PME6-010621/3916
pmi632_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI6-010621/3917
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMI6-010621/3918

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI6-010621/3919
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI6-010621/3920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PMI6-010621/3921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI6-010621/3922
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI6-010621/3923
pmi8937_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-PMI8-010621/3924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3925
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3926
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3928
pmi8952_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3929
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3931
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3932
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3933
pmi8998_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3934
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3935
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3936
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMI8-010621/3937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3938
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMI8-010621/3939
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-PMI8-010621/3940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
pmk7350_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK7-010621/3941
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK7-010621/3942
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMK7-010621/3943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK7-010621/3944
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK7-010621/3945
pmk8002_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PMK8-010621/3946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3947
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3948
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3950
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3951
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmk8003_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3953
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3954
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3956
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3957
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PMK8-010621/3958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3959
pmk8350_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3960
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3962
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PMK8-010621/3964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3965
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMK8-010621/3966
pmm6155au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PMM6-010621/3967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3968
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3969
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3971
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3972
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM6-010621/3973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmm8155au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3974
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3975
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3978
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-PMM8-010621/3979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3980
pmm8195au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3981
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3983
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PMM8-010621/3985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3986
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3987
pmm855au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-PMM8-010621/3988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3989
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3990
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3992
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3993
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmm8920au_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3995
pmm8996au_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3996
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure.	https://www.qualcomm.com/company/product-	O-QUA-PMM8-010621/3997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3998
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMM8-010621/3999
pmp8074_firmware					
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PMP8-010621/4000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMP8-010621/4001
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMP8-010621/4002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmr525_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR5-010621/4003
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR5-010621/4004
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR5-010621/4005
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-PMR5-010621/4006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR5-010621/4007
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-PMR5-010621/4008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR5-010621/4009
pmr735a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4010
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4012
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4013
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4015
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4016
pmr735b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4018
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4019
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4020
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-PMR7-010621/4021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4022
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMR7-010621/4023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
pmw3100_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMW3-010621/4024
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMW3-010621/4025
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMW3-010621/4026
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-PMW3-010621/4027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
pmx20_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4028
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4030
pmx24_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4031
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4032
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMX2-010621/4033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4034
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX2-010621/4035
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-PMX2-010621/4036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
pmx50_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4037
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4038
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMX5-010621/4039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4040
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4041
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMX5-010621/4042

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4043
pmx55_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4044
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-PMX5-010621/4045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4046
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4047
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-PMX5-010621/4048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4049
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-PMX5-010621/4050
qat3514_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4051
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4052
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4053
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QAT3-010621/4054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4055
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4056
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QAT3-010621/4057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qat3516_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4058
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4059
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QAT3-010621/4060

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4061
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4062
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4063

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4064
qat3518_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4065
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QAT3-010621/4066

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4067
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4068
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QAT3-010621/4069

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4070
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4071
qat3519_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QAT3-010621/4072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4073
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4074
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4076
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4077
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QAT3-010621/4078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qat3522_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4079
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4080
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4082
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4083
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QAT3-010621/4084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4085
qat3550_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4086
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4088
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QAT3-010621/4090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4091
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4092
qat3555_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QAT3-010621/4093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4094
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4095
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4097
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4098
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT3-010621/4099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat5515_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4100
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4101
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4103
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4104
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QAT5-010621/4105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4106
qat5516_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4107
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4109
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4110
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QAT5-010621/4111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4112
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4113
qat5522_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QAT5-010621/4114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4115
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4116
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4118
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4119
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qat5533_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4121
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4122
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4124
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4125
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QAT5-010621/4126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4127
qat5568_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4128
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4130
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QAT5-010621/4132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4133
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QAT5-010621/4134
qbt1000_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	O-QUA-QBT1-010621/4135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4136
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4137
qbt1500_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4138
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4139
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4140
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QBT1-010621/4141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4142
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT1-010621/4143
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QBT1-010621/4144

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qbt2000_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4145
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4146
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QBT2-010621/4147

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4148
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4149
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4150

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QBT2-010621/4151
qca1062_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCA1-010621/4152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
qca1064_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA1-010621/4153
qca2066_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA2-010621/4154
qca4020_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of	https://www.qualcomm.com/compa	O-QUA-QCA4-010621/4155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA4-010621/4156
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA4-010621/4157
qca4024_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QCA4-010621/4158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA4-010621/4159
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA4-010621/4160
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QCA4-010621/4161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qca6174a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4162
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4163
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4165
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4166
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca6174_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4168
qca6175a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCA6-010621/4169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4170
qca6310_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4171
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4173
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4174
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4176
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4177
qca6320_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4178

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-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4179
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4182
qca6335_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4183
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4185
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4186
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4188
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4189
qca6390_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCA6-010621/4190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4191
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4192
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4194
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4195
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6391_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4197
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4198
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4200
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4201
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QCA6-010621/4202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4203
qca6420_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4204
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4206
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4207
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4209
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4210
qca6421_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCA6-010621/4211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4212
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4213
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4215
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4216
qca6426_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCA6-010621/4217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4218
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4219
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4221
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4222
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6428_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4224
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4225
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4226

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4227
qca6430_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4228
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4230
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4231
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4233
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4234
qca6431_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-010621/4235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4236
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4237
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4239
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4240
qca6436_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA6-010621/4241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4242
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4243
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4245
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4246
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca6438_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4248
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4249
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4250

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4251
qca6564au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4252
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4254
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4257
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4258
qca6564a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4259
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4260
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4261
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4263
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4264
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-010621/4265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qca6564_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4266
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4267
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4268

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4269
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4270
qca6574au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4272
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4273
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4275
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4276
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca6574a_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4278
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4279
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4281
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4282
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QCA6-010621/4283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4284
qca6574_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4285
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4287
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4288
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4290
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4291
qca6584au_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCA6-010621/4292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4293
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4294
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA6-010621/4295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4296
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4297
qca6595au_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QCA6-010621/4298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4299
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4300
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4302
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4303
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca6595_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4305
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4306
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA6-010621/4307

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-2021-1925**	2021-bulletin	
qca6694_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4308
qca6696_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4309
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-QCA6-010621/4310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4311
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4312
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4313

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4314
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA6-010621/4315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca7500_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA7-010621/4316
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA7-010621/4317
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA7-010621/4318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca8072_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4319
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4320
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA8-010621/4321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca8075_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4322
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4323
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA8-010621/4324

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4325
qca8081_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4326
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA8-010621/4327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4328
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
qca8337_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4330
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4331
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4332
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QCA8-010621/4333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4334
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA8-010621/4335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9367_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4336
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4337
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
qca9377_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4339
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4340
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4341
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QCA9-010621/4342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4343
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4344
qca9379_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4345
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4346
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4347
qca9531_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4348
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4349
qca9558_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4350

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-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4351
qca9561_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCA9-010621/4352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4353
qca9563_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4354
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA9-010621/4355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca9880_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4357
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCA9-010621/4358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qca9882_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4359
qca9886_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4360
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCA9-010621/4361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4362
qca9887_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA9-010621/4363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4364
qca9888_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4365
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA9-010621/4366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4367
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4368
qca9889_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QCA9-010621/4369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4370
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4371
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QCA9-010621/4372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qca9896_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4373
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9898_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4375
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4376
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QCA9-010621/4377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4378
qca9980_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4379
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA9-010621/4380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4381
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4382
qca9982_firmware					
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	O-QUA-QCA9-010621/4383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4384
qca9984_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4385
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	O-QUA-QCA9-010621/4386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4387
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9985_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4389
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4390
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qca9990_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4392
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4393
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QCA9-010621/4394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4395
qca9992_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCA9-010621/4397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4398
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4399
qca9994_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QCA9-010621/4400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4401
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCA9-010621/4402
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QCA9-010621/4403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcc1110_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCC1-010621/4404
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCC1-010621/4405
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCC1-010621/4406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcm2290_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4407
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4408
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4410
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4411
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4412

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM2-010621/4413
qcm4290_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM4-010621/4414
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM4-010621/4415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM4-010621/4416
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM4-010621/4417
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCM4-010621/4418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM4-010621/4419
qcm6125_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4420
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4422
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4425
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCM6-010621/4426
qcn5021_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4427

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4428
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn5022_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4430
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4431
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN5-010621/4432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcn5024_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4433
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QCN5-010621/4434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4435
qcn5052_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4436
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCN5-010621/4437

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4438
qcn5054_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCN5-010621/4439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4440
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4441
qcn5064_firmware					
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QCN5-010621/4442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4443
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcn5121_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4445
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4446
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QCN5-010621/4447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qcn5122_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4448
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4449
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-QCN5-010621/4450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4451
qcn5124_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCN5-010621/4452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4453
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4454
qcn5152_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QCN5-010621/4455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4456
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4457
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QCN5-010621/4458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qcn5154_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4459
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QCN5-010621/4460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4461
qcn5164_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4463
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4464
qcn5500_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4465

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-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4466
qcn5502_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCN5-010621/4467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4468
qcn5550_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4469
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCN5-010621/4470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4471
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN5-010621/4472
qcn6023_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN6-010621/4473

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN6-010621/4474
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN6-010621/4475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
qcn6024_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN6-010621/4476
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN6-010621/4477
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN6-010621/4478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcn7605_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN7-010621/4479
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QCN7-010621/4480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
qcn7606_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN7-010621/4481
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN7-010621/4482
qcn9000_firmware					
Buffer Copy without	07-05-2021	7.2	Buffer overflow can occur due to improper validation	https://www.qualcomm	O-QUA-QCN9-010621/4483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	.com/company/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4484
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-QCN9-010621/4485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qcn9012_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4486
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4488
qcn9022_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4489
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4490

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4491
qcn9024_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QCN9-010621/4492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1915		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4493
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4494
qcn9070_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN9-010621/4495

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4496
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
qcn9072_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4498
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4499
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCN9-010621/4500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qcn9074_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4501
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QCN9-010621/4502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4503
qcn9100_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4504
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCN9-010621/4505

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCN9-010621/4506
qcs2290_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4507
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	O-QUA-QCS2-010621/4508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4509
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4510
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4511

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4512
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS2-010621/4513
qcs405_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4514
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4515
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4516
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCS4-010621/4517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4518
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4519
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QCS4-010621/4520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qcs410_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4521
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4522
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCS4-010621/4523

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4525
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4526

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4527
qcs4290_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4528
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QCS4-010621/4529

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4530
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4531
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QCS4-010621/4532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS4-010621/4533
qcs603_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4534
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4536
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4537
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QCS6-010621/4538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4539
qcs605_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4540
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4542
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4543
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4545
qcs610_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4546
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4547
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-QCS6-010621/4548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4549
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4550
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-QCS6-010621/4551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4552
qcs6125_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4553
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-QCS6-010621/4554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4555
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4556
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4557

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4558
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QCS6-010621/4559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qdm2301_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4560
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4561
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4562
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4564
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4565
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QDM2-010621/4566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qdm2302_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4567
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4568
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4571
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4572

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4573
qdm2305_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4574
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4576
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4577
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QDM2-010621/4578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4579
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4580
qdm2307_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4581
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4582
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4583
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4585
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4586
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QDM2-010621/4587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qdm2308_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4588
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4589
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4590

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4592
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4593

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4594
qdm2310_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4595
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM2-010621/4596

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4597
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4598
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QDM2-010621/4599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4600
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM2-010621/4601
qdm3301_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4602
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4603
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4604
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM3-010621/4605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4606
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4607
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QDM3-010621/4608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qdm3302_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4609
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4610
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QDM3-010621/4611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4612
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM3-010621/4613
qdm4643_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QDM4-010621/4614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4615
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4616
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4618
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4619
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm4650_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4621
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4622
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4624
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4625
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QDM4-010621/4626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM4-010621/4627
qdm5579_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4628
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4630
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4631
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-QDM5-010621/4632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5620_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4633
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4634
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4636
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4637
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QDM5-010621/4638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4639
qdm5621_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4640
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4642
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4643
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4645
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4646
qdm5650_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4648
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4649
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4650
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QDM5-010621/4651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4652
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5652_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4654
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4655
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4657
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4658
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QDM5-010621/4659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4660
qdm5670_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4661
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4663
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4664
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4666
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4667
qdm5671_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4669
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4670
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4671
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QDM5-010621/4672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4673
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qdm5677_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4675
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4676
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4678
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4679
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QDM5-010621/4680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4681
qdm5679_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4682
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4684
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4685
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4687
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QDM5-010621/4688
qet4100_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4690
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4691
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4692
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QET4-010621/4693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4694
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qet4101_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4696
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4697
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4698
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-QET4-010621/4699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4700
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QET4-010621/4701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4702
qet4200aq_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET4-010621/4703
qet5100m_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QET5-010621/4704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4705
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4706
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4708
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4709
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qet5100_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4711
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4712
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4714
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4715
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QET5-010621/4716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET5-010621/4717
qet6100_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4718
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4720
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QET6-010621/4722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4723
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4724
qet6105_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QET6-010621/4725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4726
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4727
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4729
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4730
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qet6110_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4732
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4733
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4735
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4736
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QET6-010621/4737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QET6-010621/4738
qfe2080fc_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-010621/4739
qfe2081fc_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-010621/4740
qfe2082fc_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4741
qfe2101_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QFE2-020621/4742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4743
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4744
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4746
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4747
qfe2520_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4749
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4750
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4751
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QFE2-020621/4752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qfe2550_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4753
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4754
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QFE2-020621/4755

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4756
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE2-020621/4757
qfe3100_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QFE3-020621/4758

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-2021-1905**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4759
qfe3340_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4760
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4762
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4763
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe3440fc_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE3-020621/4765
qfe4301_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4766
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4768
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4769
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
qfe4302_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4771
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4772
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4773
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QFE4-020621/4774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4775
qfe4303_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4776
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4778
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4779
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe4305_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4781
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4782
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4783
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-QFE4-020621/4784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4785
qfe4308_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4786
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QFE4-020621/4787

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4788
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4789
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe4309_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4791
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4792
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4794
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4795
qfe4320_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4796
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QFE4-020621/4797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4798
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4799
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfe4373fc_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4801
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4802
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4804
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4805
qfe4455fc_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QFE4-020621/4806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
qfe4465fc_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFE4-020621/4807
qfs2530_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4808
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4810
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4811
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QFS2-020621/4812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4813
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4814
qfs2580_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QFS2-020621/4815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4816
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4817
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4819
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4820
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qfs2608_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4822
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4823
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4825
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4826
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QFS2-020621/4827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4828
qfs2630_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4829
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4831
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4832
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QFS2-020621/4833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4834
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QFS2-020621/4835
qln1020_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QLN1-020621/4836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4837
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4838
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4840
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4841
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qln1021aq_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4843
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QLN1-020621/4845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4846
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4847
qln1030_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QLN1-020621/4848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4849
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4850
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4852
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4853
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QLN1-020621/4854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qln1031_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4855
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QLN1-020621/4857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4858
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4859
qln1035bd_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4860
qln1036aq_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4861
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4862
Buffer Copy without Checking	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application	https://www.qualcomm.com/compa	O-QUA-QLN1-020621/4863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	ny/product-security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4864
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN1-020621/4865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qln4640_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4866
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4867
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4869
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4870
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-QLN4-020621/4871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4872
qln4642_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4873
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4875
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4876
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4878
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4879
qln4650_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4881
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4882
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4883
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QLN4-020621/4884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4885
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN4-020621/4886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qln5020_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4887
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4888
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4889
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-QLN5-020621/4890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4891
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QLN5-020621/4892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4893
qln5030_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4894
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4896
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4899
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4900
qln5040_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4902
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4903
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4904
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QLN5-020621/4905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4906
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QLN5-020621/4907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpa2625_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA2-020621/4908
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA2-020621/4909
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA2-020621/4910
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-QPA2-020621/4911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA2-020621/4912
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QPA2-020621/4913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA2-020621/4914
qpa4340_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4915
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4917
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4918
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4920
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4921
qpa4360_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4923
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4924
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4925
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-QPA4-020621/4926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4927
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpa4361_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4929
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4930
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4931
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-QPA4-020621/4932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4933
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-QPA4-020621/4934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA4-020621/4935
qpa5373_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4936
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4938
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4939
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4940
qpa5460_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4941
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4942
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4943
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-QPA5-020621/4944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4945
qpa5461_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4946
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-QPA5-020621/4947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4948
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4949
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4950

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4951
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qpa5580_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4953
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4954
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4955
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA5-020621/4956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4957
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4958
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QPA5-020621/4959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qpa5581_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4960
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4961
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA5-020621/4962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4964
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA5-020621/4965

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA5-020621/4966
qpa6560_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA6-020621/4967
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA6-020621/4968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA6-020621/4969
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA6-020621/4970
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPA6-020621/4971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA6-020621/4972
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA6-020621/4973
qpa8673_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4974
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4975
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4976
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/4977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4978
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4979
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QPA8-020621/4980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpa8675_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4981
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4982
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/4983

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4985
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4986

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4987
qpa8686_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4988
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/4989

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4990
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4991
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPA8-020621/4992

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4993
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4994
qpa8688_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group	https://www.qualcomm.com/compa	O-QUA-QPA8-020621/4995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	ny/product-security/bulletins/may-2021-bulletin	
qpa8801_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4996
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4997
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QPA8-020621/4998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	letins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/4999
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5000
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/5001

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5002
qpa8802_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5003
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/5004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5005
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5006
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5007

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5008
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5009
qpa8803_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5010
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5011
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5012
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/5013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5014
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5015
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QPA8-020621/5016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpa8821_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5017
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5018
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/5019

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5021
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5022

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5023
qpa8842_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5024
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPA8-020621/5025

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5026
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPA8-020621/5028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5029
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPA8-020621/5030
qpm2630_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QPM2-020621/5031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM2-020621/5032
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM2-020621/5033
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM2-020621/5034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM2-020621/5035
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM2-020621/5036
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM2-020621/5037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm4621_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5038
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5039
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5041
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5042
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QPM4-020621/5043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5044
qpm4630_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5045
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5047
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM4-020621/5049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5050
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5051
qpm4640_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QPM4-020621/5052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5053
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5054
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5056
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5057
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qpm4641_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5059
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5060
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5062
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5063
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QPM4-020621/5064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5065
qpm4650_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5066
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5068
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5069
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM4-020621/5070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5071
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM4-020621/5072
qpm5541_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QPM5-020621/5073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5074
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5075
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM5-020621/5076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5077
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5078
qpm5577_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QPM5-020621/5079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5080
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5081
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5082

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5083
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5084
qpm5579_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5085
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5086
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5087
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5088

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5089
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
qpm5620_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5091
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5092
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5093
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QPM5-020621/5094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5095
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5097
qpm5621_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5098
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5099
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-QPM5-020621/5100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5101
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5102
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-QPM5-020621/5103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5104
qpm5641_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5105
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-QPM5-020621/5106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5107
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5108
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5109

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5110
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qpm5657_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5112
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5113
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5114
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5116
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5117
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QPM5-020621/5118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qpm5658_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5119
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5120
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5122
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5123
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5124

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5125
qpm5670_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5126
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5128
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM5-020621/5130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5131
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5132
qpm5677_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5133
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5134
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5135
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5137
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5138
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QPM5-020621/5139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpm5679_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5140
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5141
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5142

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5143
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5144
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5145

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5146
qpm5870_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5147
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5148

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5149
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5150
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM5-020621/5151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5152
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5153
qpm5875_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QPM5-020621/5154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5155
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5156
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5158
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM5-020621/5159
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM5-020621/5160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm6325_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5161
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5162
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5164
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5165
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QPM6-020621/5166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	letins/may-2021-bulletin	
qpm6375_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5167
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5168
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5170
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5171
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-QPM6-020621/5172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
qpm6582_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5173
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5174
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5176
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5177
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5178

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5179
qpm6585_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5180
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5182
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM6-020621/5184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5185
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5186
qpm6621_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5187
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5188
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5189
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5191
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5192
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QPM6-020621/5193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qpm6670_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5194
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5195
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM6-020621/5196

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5197
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5198
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5199

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM6-020621/5200
qpm8820_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5201
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM8-020621/5202

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5203
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5204
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM8-020621/5205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5206
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5207
qpm8830_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QPM8-020621/5208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5209
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5210
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5212
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5213
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QPM8-020621/5214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qpm8870_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5215
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5216
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5218
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5219
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-QPM8-020621/5220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5221
qpm8895_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5222
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5224
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5225
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QPM8-020621/5226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5227
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QPM8-020621/5228
qsm7250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-QSM7-020621/5229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5230
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5231
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5233
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5234
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM7-020621/5235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
qsm8250_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM8-020621/5236
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSM8-020621/5237
qsm8350_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper	https://www.qualcomm	O-QUA-QSM8-020621/5238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	.com/company/product-security/bulletins/may-2021-bulletin	
qsw6310_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW6-020621/5239
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW6-020621/5240
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure.	https://www.qualcomm.com/company/product-	O-QUA-QSW6-020621/5241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW6-020621/5242
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW6-020621/5243
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QSW6-020621/5244

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-2021-1925**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW6-020621/5245
qsw8573_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5246
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	O-QUA-QSW8-020621/5247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5248
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5250

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5251
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5252
qsw8574_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5253
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5254
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5255
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QSW8-020621/5256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5257
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QSW8-020621/5258
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-QSW8-020621/5259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
qtc410s_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5260
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5261
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QTC4-020621/5262

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5263
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5264
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5265

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC4-020621/5266
qtc800h_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5267
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QTC8-020621/5268

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5269
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5270
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QTC8-020621/5271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5272
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5273
qtc800s_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QTC8-020621/5274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5275
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5276
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5278
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5279
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QTC8-020621/5280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
qtc800t_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5281
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5282
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-QTC8-020621/5283

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-2021-1925**	letins/may-2021-bulletin	
qtc801s_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5284
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5285
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QTC8-020621/5286

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5288
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5289

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTC8-020621/5290
qtm525_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5291
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QTM5-020621/5292

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5293
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5294
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-QTM5-020621/5295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5296
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5297
qtm527_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-QTM5-020621/5298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5299
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5300
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5301

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5302
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QTM5-020621/5303
qualcomm215_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QUAL-020621/5304
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QUAL-020621/5305
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QUAL-020621/5306
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-QUAL-020621/5307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-QUAL-020621/5308
rgr7640au_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RGR7-020621/5309
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-RGR7-020621/5310

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RGR7-020621/5311
rsw8577_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5312
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5314
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5315
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5317
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-RSW8-020621/5318
sa2150p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA21-020621/5319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA21-020621/5320
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA21-020621/5321
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SA21-020621/5322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA21-020621/5323
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA21-020621/5324
sa415m_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SA41-020621/5325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA41-020621/5326
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA41-020621/5327
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA41-020621/5328

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA41-020621/5329
sa515m_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA51-020621/5330
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA51-020621/5331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA51-020621/5332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA51-020621/5333
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA51-020621/5334

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA51-020621/5335
sa6145p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5336
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA61-020621/5337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5338
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5339
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SA61-020621/5340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5341
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5342
sa6150p_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5343
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5344
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5345
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA61-020621/5346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5347
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5348
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-SA61-020621/5349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
sa6155p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5350
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5351
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA61-020621/5352

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5353
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5354
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5355

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5356
sa6155_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5357
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA61-020621/5358

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5359
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5360
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SA61-020621/5361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5362
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA61-020621/5363
sa8150p_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-SA81-020621/5364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5365
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5366
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5368
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5369
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SA81-020621/5370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
sa8155p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5371
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5372
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5374
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5375
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SA81-020621/5376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5377
sa8155_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5378
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5380
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5381
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SA81-020621/5382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5383
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5384
sa8195p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SA81-020621/5385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5386
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5387
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5389
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5390
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SA81-020621/5391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sc8180x\\+sdx55_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SC81-020621/5392
sd205_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD20-020621/5393
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD20-020621/5394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD20-020621/5395
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD20-020621/5396
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-SD20-020621/5397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd210_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD21-020621/5398
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD21-020621/5399
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD21-020621/5400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD21-020621/5401
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD21-020621/5402
sd429_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD42-020621/5403
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD42-020621/5404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD42-020621/5405
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD42-020621/5406
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD42-020621/5407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd439_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD43-020621/5408
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD43-020621/5409
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD43-020621/5410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD43-020621/5411
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD43-020621/5412
sd450_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5413
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-SD45-020621/5414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5415
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5416
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd455_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5418
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5419
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD45-020621/5420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD45-020621/5421
sd460_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5422
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5424
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5425
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD46-020621/5426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5427
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD46-020621/5428
sd480_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SD48-020621/5429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5430
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5431
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5433
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5434
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD48-020621/5435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd632_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5436
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5437
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5439
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5440
sd636_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5442
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5443
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD63-020621/5444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD63-020621/5445
sd660_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5446
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5448
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5449
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD66-020621/5450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5451
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5452
sd662_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SD66-020621/5453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5454
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5455
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5457
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5458
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd665_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5460
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5461
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5463
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5464
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SD66-020621/5465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD66-020621/5466
sd670_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5467
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5469
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5470
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD67-020621/5471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5472
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5473
sd675_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SD67-020621/5474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5475
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5476
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5478
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5479
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd678_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5481
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5482
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5484
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5485
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SD67-020621/5486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD67-020621/5487
sd6905g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5488
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5490
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5491
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD69-020621/5492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5493
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD69-020621/5494
sd710_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SD71-020621/5495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5496
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5497
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5499
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5500
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd712_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD71-020621/5502
sd720g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD72-020621/5503
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD72-020621/5504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD72-020621/5505
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD72-020621/5506
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD72-020621/5507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD72-020621/5508
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD72-020621/5509
sd730_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD73-020621/5510
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD73-020621/5511
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD73-020621/5512
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD73-020621/5513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD73-020621/5514
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD73-020621/5515
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-SD73-020621/5516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
sd750g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5517
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5518
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD75-020621/5519

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5520
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5521
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5522

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD75-020621/5523
sd765g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5524
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD76-020621/5525

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5526
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5527
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD76-020621/5528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5529
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5530
sd765_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-SD76-020621/5531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5532
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5533
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5535
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5536
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD76-020621/5537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
sd768g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5538
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5539
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5542
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SD76-020621/5543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD76-020621/5544
sd7c_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD7C-020621/5545
sd835_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD83-020621/5546
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD83-020621/5547
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD83-020621/5548
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SD83-020621/5549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD83-020621/5550
sd845_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD84-020621/5551
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of	https://www.qualcomm.com/compa	O-QUA-SD84-020621/5552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	ny/product-security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD84-020621/5553
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD84-020621/5554
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SD84-020621/5555

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD84-020621/5556
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD84-020621/5557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
sd850_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5558
sd855_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5559
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5561
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5562
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5564
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD85-020621/5565
sd8655g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5567
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5568
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5569
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SD86-020621/5570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5571
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD86-020621/5572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sd870_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD87-020621/5573
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD87-020621/5574
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD87-020621/5575
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-SD87-020621/5576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD87-020621/5577
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-SD87-020621/5578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD87-020621/5579
sd8885g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5580
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5582
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5583
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5585
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5586
sd888_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5588
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5589
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5590
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SD88-020621/5591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD88-020621/5592
sd8cx_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5593
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-SD8C-020621/5594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5595
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5596
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper	https://www.qualcomm	O-QUA-SD8C-020621/5597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	.com/company/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5598
sd8c_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5600
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5601
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SD8C-020621/5602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5603
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SD8C-020621/5604
sda429w_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SDA4-020621/5605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDA4-020621/5606
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDA4-020621/5607
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDA4-020621/5608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDA4-020621/5609
sdm429w_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM4-020621/5610
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM4-020621/5611
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-SDM4-020621/5612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM4-020621/5613
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM4-020621/5614
sdm630_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-SDM6-020621/5615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM6-020621/5616
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM6-020621/5617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM6-020621/5618

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM6-020621/5619
sdm830_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM8-020621/5620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM8-020621/5621
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM8-020621/5622
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM8-020621/5623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDM8-020621/5624
sdr051_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5625
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5626
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-SDR0-020621/5627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5628
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5629
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-SDR0-020621/5630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5631
sdr052_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5632
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-SDR0-020621/5633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5634
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5636

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5637
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR0-020621/5638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdr425_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR4-020621/5639
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR4-020621/5640
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR4-020621/5641
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR4-020621/5642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR4-020621/5643
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR4-020621/5644
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-SDR4-020621/5645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
sdr660g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5646
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5647
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR6-020621/5648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5649
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5650
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR6-020621/5651

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5652
sdr660_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5653
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR6-020621/5654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
sImproper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5655
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5656
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SDR6-020621/5657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5658
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5659
sdr675_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5660
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5661
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5662
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR6-020621/5663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5664
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR6-020621/5665
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-SDR6-020621/5666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
sdr735g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5667
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5668
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR7-020621/5669

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5670
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5671
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5672

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5673
sdr735_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5674
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR7-020621/5675

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5676
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5677
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SDR7-020621/5678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5679
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR7-020621/5680
sdr8150_firmware					
Integer Overflow or	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an	https://www.qualcomm.com/compa	O-QUA-SDR8-020621/5681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	ny/product-security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5682
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5683
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5685
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5686
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDR8-020621/5687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	2021-bulletin	
sdr8250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5688
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5689
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5691
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5692
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SDR8-020621/5693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5694
sdr845_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5695
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5697
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5698
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-SDR8-020621/5699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sdr865_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5700
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5701
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5704
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-SDR8-020621/5705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDR8-020621/5706
sdw2500_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDW2-020621/5707
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SDW2-020621/5708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
sdw3100_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDW3-020621/5709
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDW3-020621/5710
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDW3-020621/5711
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while	https://www.qualcomm	O-QUA-SDW3-020621/5712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	.com/company/product-security/bulletins/may-2021-bulletin	
sdx20m_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5713
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5715
sdx20_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5716
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5717
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto,	https://www.qualcomm.com/compa	O-QUA-SDX2-020621/5718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	ny/product-security/bulletins/may-2021-bulletin	
sdx24_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5719
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5720
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX2-020621/5722
sdx50m_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5723
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5725
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5726
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5728
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5729
sdx55m_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5731
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5732
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5733
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SDX5-020621/5734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5735
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sdx55_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5737
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5738
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5739
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-SDX5-020621/5740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5741
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-SDX5-020621/5742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDX5-020621/5743
sdxr1_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5744
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5746
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5747
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5749
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5750
sdxr25g_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5752
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5755
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5756
sdxr2_5g_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SDXR-020621/5757

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-2021-1905**		
sm4125_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5758
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5759
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1906		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5762
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SM41-020621/5763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM41-020621/5764
sm6250p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5765
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5767
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5768
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SM62-020621/5769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5770
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5771
sm6250_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-SM62-020621/5772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5773
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5774
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5776
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5777
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM62-020621/5778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
sm7250p_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5779
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5780
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5782
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5783
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-SM72-020621/5784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM72-020621/5785
sm7350_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM73-020621/5786
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM73-020621/5787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM73-020621/5788
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SM73-020621/5789
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver 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/may-2021-bulletin	O-QUA-SM73-020621/5790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1350_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5791
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5792
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**		
smb1351_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5794
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5795
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5796
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-SMB1-020621/5797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5798
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-SMB1-020621/5799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5800
smb1354_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5801
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5803
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5804
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5806
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5807
smb1355_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5809
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5810
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5811
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SMB1-020621/5812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5813
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1357_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5815
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5816
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1910		
smb1358_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5818
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5819
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5820
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SMB1-020621/5821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5822
smb1360_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5823
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5825
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5826
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1380_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5828
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5829
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5830
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length	https://www.qualcomm	O-QUA-SMB1-020621/5831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	.com/company/product-security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5832
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-SMB1-020621/5833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5834
smb1381_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5835
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5837
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5838
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5840
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5841
smb1390_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5843
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5844
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5845
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-SMB1-020621/5846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5847
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
smb1394_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5849
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5850
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5851
Buffer Copy without Checking Size of Input ('Classic	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bul	O-QUA-SMB1-020621/5852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5853
smb1395_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5854
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in	https://www.qualcomm.com/company/product-security/bul	O-QUA-SMB1-020621/5855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	letins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5856
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5857
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5858

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5859
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5860
smb1396_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5861
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5862
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5863
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMB1-020621/5864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5865
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5866
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-SMB1-020621/5867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
smb1398_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5868
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5869
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMB1-020621/5870

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5871
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5872
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5873

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB1-020621/5874
smb231_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5876
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5877
smb2351_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5878
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5880
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5881
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMB2-020621/5882

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB2-020621/5883
smb358s_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB3-020621/5884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMB3-020621/5885
smr525_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5886
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5887
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMR5-020621/5888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5889
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5890
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMR5-020621/5891

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-2021-1925**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5892
smr526_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5893
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMR5-020621/5894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5895
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5896
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-SMR5-020621/5897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5898
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5899
smr545_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5900
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5901
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5902
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMR5-020621/5903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5904
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5905
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-SMR5-020621/5906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
smr546_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5907
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5908
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-SMR5-020621/5909

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5910
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5911
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5912

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-SMR5-020621/5913
wcd9326_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5914
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCD9-020621/5915

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5916
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5917
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCD9-020621/5918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5919
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5920
wcd9330_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5921
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5922
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5923
wcd9335_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5924
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5925
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5926
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCD9-020621/5927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5928
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5929
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-WCD9-020621/5930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wcd9340_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5931
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5932
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCD9-020621/5933

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5935
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5936

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5937
wcd9341_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5938
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCD9-020621/5939

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-2021-1905**	2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5940
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5941
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCD9-020621/5942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5943
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5944
wcd9360_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5945
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5946
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5947
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCD9-020621/5948

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-2021-1915**	2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5949
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wcd9370_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5951
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5952
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5953
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WCD9-020621/5954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5955
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5957
wcd9371_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5958
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5960
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5963
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5964
wcd9375_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5966
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5967
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5968
Buffer Copy without Checking Size of Input	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in	https://www.qualcomm.com/company/product-	O-QUA-WCD9-020621/5969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	security/bulletins/may-2021-bulletin	
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5970
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcd9380_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5972
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5973
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5975
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5976
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-WCD9-020621/5977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5978
wcd9385_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5979
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5981
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5982
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5984
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCD9-020621/5985
wcn3610_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5987
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5988
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5989
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-WCN3-020621/5990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wcn3615_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5991
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5992
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCN3-020621/5993

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5994
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5995
wcn3620_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCN3-020621/5996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1895	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5997
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5998
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/5999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6000
wcn3660b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6001
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6003
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6004
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6005
wcn3660_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6006
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6007
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6008
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCN3-020621/6009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6010
wcn3680b_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6011
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6013
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6014
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wcn3680_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6016
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6017
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6018
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WCN3-020621/6019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6020
wcn3910_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6021
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6023
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6024
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCN3-020621/6025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6026
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6027
wcn3950_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-WCN3-020621/6028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6029
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6030
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6032
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6033
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn3980_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6035
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6036
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6039
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-WCN3-020621/6040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6041
wcn3988_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6042
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6044
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6045
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCN3-020621/6046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6047
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6048
wcn3990_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-WCN3-020621/6049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6050
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6051
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6053
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6054
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn3991_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6056
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6057
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6059
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6060
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-WCN3-020621/6061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6062
wcn3998_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6063
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6065
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6066
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCN3-020621/6067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6068
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6069
wcn3999_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bul	O-QUA-WCN3-020621/6070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	letins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6071
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6072
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6074
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6075
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN3-020621/6076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wcn6740_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6077
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6078
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6080
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6081
wcn6745_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6082

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-2021-1925**		
wcn6750_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6083
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6084
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCN6-020621/6085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
wcn6850_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6086
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6087
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6090
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame 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/may-2021-bulletin	O-QUA-WCN6-020621/6091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6092
wcn6851_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6093
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1905		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6095
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6096
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6098
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6099
wcn6855_firmware					
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6100

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-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6101
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6102
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length 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/may-2021-bulletin	O-QUA-WCN6-020621/6103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6104
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6105
wcn6856_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6106
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6107
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6108
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WCN6-020621/6109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6110
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WCN6-020621/6111
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in	https://www.qualcomm.com/company/product-	O-QUA-WCN6-020621/6112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	security/bulletins/may-2021-bulletin	
wgr7640_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6113
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6114
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WGR7-020621/6115

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-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6116
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6117
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6118

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-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WGR7-020621/6119
whs9410_firmware					
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, 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/may-2021-bulletin	O-QUA-WHS9-020621/6120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1925		
wsa8810_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6121
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6122
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6123
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WSA8-020621/6124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6125
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6127
wsa8815_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6128
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6129
Improper Handling of	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU	https://www.qualcomm.com/compa	O-QUA-WSA8-020621/6130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	ny/product-security/bulletins/may-2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6132
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame	https://www.qualcomm.com/company/product-	O-QUA-WSA8-020621/6133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	security/bulletins/may-2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6134
wsa8830_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6135
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes	https://www.qualcomm.com/company/product-	O-QUA-WSA8-020621/6136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	security/bulletins/may-2021-bulletin	
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6137
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6138
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6139

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-2021-1915**		
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6140
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8835_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6142
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6143
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6144
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WSA8-020621/6145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6146
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WSA8-020621/6147
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in	https://www.qualcomm.com/compa	O-QUA-WSA8-020621/6148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	ny/product-security/bulletins/may-2021-bulletin	
wtr2955_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6149
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6150
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WTR2-020621/6151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	2021-bulletin	
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6152
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6153
wtr2965_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/may-	O-QUA-WTR2-020621/6154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	2021-bulletin	
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6155
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6156
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6158
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6159
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR2-020621/6160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**		
wtr3925_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6161
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6162
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**		
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6165
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action 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/may-2021-bulletin	O-QUA-WTR3-020621/6166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**		
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR3-020621/6167
wtr4905_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR4-020621/6168
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR4-020621/6169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**		
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR4-020621/6170
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR4-020621/6171
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR4-020621/6172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1927		
wtr5975_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6173
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6174
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6175
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-WTR5-020621/6176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	security/bulletins/may-2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6177
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR5-020621/6179
wtr6955_firmware					
Integer Overflow or Wraparound	07-05-2021	7.2	Possible integer overflow due to improper length check while flashing an image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music **CVE ID : CVE-2021-1895**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6180
Use After Free	07-05-2021	7.2	Possible use after free due to improper handling of memory mapping of multiple processes simultaneously. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1905**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Handling of Exceptional Conditions	07-05-2021	2.1	Improper handling of address deregistration on failure can lead to new GPU address allocation failure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1906**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6182
Double Free	07-05-2021	10	Double free in video due to lack of input buffer length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1910**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6183
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-05-2021	7.2	Buffer overflow can occur due to improper validation of NDP application information length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1915**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-05-2021	7.8	Possible denial of service scenario due to improper handling of group management action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1925**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6185
Use After Free	07-05-2021	7.2	Possible use after free due to lack of null check while memory is being freed in FastRPC driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1927**	https://www.qualcomm.com/company/product-security/bulletins/may-2021-bulletin	O-QUA-WTR6-020621/6186
Redhat					
enterprise_linux					
Out-of-bounds Write	06-05-2021	3.6	A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an array index, which can be updated by a user process	https://bugzilla.redhat.com/show_bug.cgi?id=1950136, https://git.kernel.org/pu	O-RED-ENTE-020621/6187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			at anytime which could lead to an out-of-bounds write. The highest threat from this vulnerability is to data integrity and system availability. **CVE ID : CVE-2021-3501**	b/scm/linux/kernel/git/torvalds/linux.git/commit/?id=04c4f2ee3f68c9a4bf1653d15f1a9a435ae33f7a	
Out-of-bounds Read	05-05-2021	5.5	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity. **CVE ID : CVE-2021-20254**	https://www.samba.org/samba/security/CVE-2021-20254.html	O-RED-ENTE-020621/6188
Suse					
linux_enterprise_server					
Incorrect Default Permissions	05-05-2021	2.1	A Incorrect Default Permissions vulnerability in the packaging of cups of SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Manager Server 4.0, SUSE OpenStack Cloud Crowbar 9; openSUSE Leap 15.2, Factory allows local	https://bugzilla.suse.com/show_bug.cgi?id=1184161	O-SUS-LINU-020621/6189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers with control of the lp users to create files as root with 0644 permissions without the ability to set the content. This issue affects: SUSE Linux Enterprise Server 11-SP4-LTSS cups versions prior to 1.3.9. SUSE Manager Server 4.0 cups versions prior to 2.2.7. SUSE OpenStack Cloud Crowbar 9 cups versions prior to 1.7.5. openSUSE Leap 15.2 cups versions prior to 2.2.7. openSUSE Factory cups version 2.3.3op2-2.1 and prior versions. **CVE ID : CVE-2021-25317**		
Tenda					
ac11_firmware					
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setmac allows attackers to execute arbitrary code on the system via a crafted post request. **CVE ID : CVE-2021-31755**	N/A	O-TEN-AC11-020621/6190
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /gofrom/setwanType allows attackers to execute	N/A	O-TEN-AC11-020621/6191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on the system via a crafted post request. This occurs when input vector controlled by malicious attack get copied to the stack variable. **CVE ID : CVE-2021-31756**		
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setVLAN allows attackers to execute arbitrary code on the system via a crafted post request. **CVE ID : CVE-2021-31757**	N/A	O-TEN-AC11-020621/6192
Out-of-bounds Write	07-05-2021	10	An issue was discovered on Tenda AC11 devices with firmware through 02.03.01.104_CN. A stack buffer overflow vulnerability in /goform/setportList allows attackers to execute arbitrary code on the system via a crafted post request. **CVE ID : CVE-2021-31758**	N/A	O-TEN-AC11-020621/6193