



National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Nov 2019

Vol. 06 No. 22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Apache					
atlas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Apache Atlas versions 0.8.3 and 1.1.0 were found vulnerable to Stored Cross-Site Scripting in the search functionality CVE ID : CVE-2019-10070	N/A	A-APA-ATLA-031219/1
nifi					
Improper Restriction of XML External Entity Reference ('XXE')	19-11-2019	4	The XMLFileLookupService in NiFi versions 1.3.0 to 1.9.2 allowed trusted users to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE) and reveal information such as the versions of Java, Jersey, and Apache that the NiFi instance uses. CVE ID : CVE-2019-10080	https://nifi.apache.org/security.html#CVE-2019-10080	A-APA-NIFI-031219/2
Information Exposure	19-11-2019	5	When updating a Process Group via the API in NiFi versions 1.3.0 to 1.9.2, the response to the request includes all of its contents (at the top most level, not recursively). The response included details about processors and controller	https://nifi.apache.org/security.html#CVE-2019-10083	A-APA-NIFI-031219/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			services which the user may not have had read access to. CVE ID : CVE-2019-10083							
Insufficient Session Expiration	19-11-2019	6.5	When using an authentication mechanism other than PKI, when the user clicks Log Out in NiFi versions 1.0.0 to 1.9.2, NiFi invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi. CVE ID : CVE-2019-12421	https://nifi.apache.org/security.html#CVE-2019-12421	A-APA-NIFI-031219/4					
solr										
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	The 8.1.1 and 8.2.0 releases of Apache Solr contain an insecure setting for the ENABLE_REMOTE_JMX_OPTS configuration option in the default solr.in.sh configuration file shipping with Solr. If you use the default solr.in.sh file from the affected releases, then JMX monitoring will be enabled and exposed on RMI_PORT (default=18983), without any authentication. If this port is opened for inbound traffic in your firewall, then anyone with network access to your Solr nodes will be able to access JMX, which may in turn allow them to upload malicious code for execution	N/A	A-APA-SOLR-031219/5					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the Solr server. CVE ID : CVE-2019-12409		
shiro					
Improper Input Validation	18-11-2019	5	Apache Shiro before 1.4.2, when using the default "remember me" configuration, cookies could be susceptible to a padding attack. CVE ID : CVE-2019-12422	N/A	A-APA-SHIR-031219/6
Centreon					
centreon_web					
Incorrect Permission Assignment for Critical Resource	21-11-2019	7.2	Centreon Web 19.04.4 has weak permissions within the OVA (aka VMware virtual machine) and OVF (aka VirtualBox virtual machine) files, allowing attackers to gain privileges via a Trojan horse Centreon-autodisco executable file that is launched by cron. CVE ID : CVE-2019-16406	N/A	A-CEN-CENT-031219/7
cloudfoundry					
cf-deployment					
Improper Input Validation	19-11-2019	7.8	Cloud Foundry Routing, all versions before 0.193.0, does not properly validate nonce input. A remote unauthorized malicious user could forge a route service request using an invalid nonce that will cause the Gorouter to crash. CVE ID : CVE-2019-11289	https://www.cloudfoundry.org/blog/cve-2019-11289	A-CLO-CF-D-031219/8
routing-release					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	19-11-2019	7.8	Cloud Foundry Routing, all versions before 0.193.0, does not properly validate nonce input. A remote unauthorized malicious user could forge a route service request using an invalid nonce that will cause the Gorouter to crash. CVE ID : CVE-2019-11289	https://www.cloudfoundry.org/blog/cve-2019-11289	A-CLO-ROUT-031219/9
code42					
code42					
Untrusted Search Path	19-11-2019	6.9	Code42 app through version 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a non-administrative attacker on the local machine could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local machine. CVE ID : CVE-2019-16860	https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_security_advisories/Arbitrary_code_execution_on_local_Windows_devices	A-COD-CODE-031219/10
Untrusted Search Path	19-11-2019	6.9	Code42 server through 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a non-administrative attacker on the local server could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the	https://code42.com/r/support/CVE-2019-16861	A-COD-CODE-031219/11

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			local server. CVE ID : CVE-2019-16861							
Codesys										
control_for_plcnext										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/12					
control_for_beaglebone										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/13					
control_for_empc-a\imx6										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/14					
control_for_iot2000										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/15					
control_for_linux										
Buffer Copy	20-11-2019	7.5	CODESYS 3 web server	N/A	A-COD-CONT-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858		031219/16
control_for_pfc100					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/17
control_for_pfc200					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/18
control_for_raspberry_pi					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/19
control_rte					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/20

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
control_runtime_system_toolkit										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/21					
control_win										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-CONT-031219/22					
embedded_target_visu_toolkit										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-EMBE-031219/23					
hmi										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow. CVE ID : CVE-2019-18858	N/A	A-COD-HMI-031219/24					
remote_target_visu_toolkit										
Buffer Copy without Checking Size of Input ('Classic	20-11-2019	7.5	CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.	N/A	A-COD-REMO-031219/25					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer Overflow')			CVE ID : CVE-2019-18858							
Comodo										
comodo_internet_security										
Untrusted Search Path	18-11-2019	4.4	An issue was discovered in signmgr.dll 6.5.0.819 in Comodo Internet Security through 12.0. A DLL Preloading vulnerability allows an attacker to implant an unsigned DLL named iLog.dll in a partially unprotected product directory. This DLL is then loaded into a high-privileged service before the binary signature validation logic is loaded, and might bypass some of the self-defense mechanisms. CVE ID : CVE-2019-18215	N/A	A-COM-COMO-031219/26					
Fasterxml										
jackson-mapper-asl										
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes. CVE ID : CVE-2019-10172	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10172	A-FAS-JACK-031219/27					
footy										
tipping_software										
Improper Neutralization of Input	18-11-2019	4.3	Footy Tipping Software AFL Web Edition 2019 allows	N/A	A-FOO-TIPP-031219/28					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			XSS. CVE ID : CVE-2019-17057		
Unrestricted Upload of File with Dangerous Type	18-11-2019	6.5	Footy Tipping Software AFL Web Edition 2019 allows arbitrary file upload and resultant remote code execution because a whitelist can be bypassed by an Administrator who uploads a crafted upload.dat file. CVE ID : CVE-2019-17058	N/A	A-FOO-TIPP-031219/29
Fortinet					
forticlient					
Information Exposure	21-11-2019	2.1	A clear text storage of sensitive information vulnerability in FortiClient for Mac may allow a local attacker to read sensitive information logged in the console window when the user connects to an SSL VPN Gateway. CVE ID : CVE-2019-15704	https://fortiguard.com/advisory/FG-IR-19-227	A-FOR-FORT-031219/30
getmailbird					
mailbird					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Mailbird before 2.7.5.0 r allow remote attackers to execute arbitrary JavaScript in a privileged context via a crafted HTML mail message. This vulnerability is distinct from CVE-2015-4657.	https://www.getmailbird.com/ReleaseNotes/LatestReleaseNotes.html	A-GET-MAIL-031219/31

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-15054		
GNU					
serveez					
Information Exposure	20-11-2019	5	<p>GNU Serveez through 0.2.2 has an Information Leak. An attacker may send an HTTP POST request to the /cgi-bin/reader URI. The attacker must include a Content-length header with a large positive value that, when represented in 32 bit binary, evaluates to a negative number. The problem exists in the http_cgi_write function under http-cgi.c; however, exploitation might show svz_envblock_add in libserveez/passthrough.c as the location of the heap-based buffer over-read.</p> <p>CVE ID : CVE-2019-16200</p>	N/A	A-GNU-SERV-031219/32
Google					
chrome					
Use After Free	25-11-2019	4.3	<p>Use after free in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.</p> <p>CVE ID : CVE-2019-5860</p>	N/A	A-GOO-CHRO-031219/33
Use After Free	25-11-2019	4.3	<p>Use after free in PDFium in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF</p>	N/A	A-GOO-CHRO-031219/34

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. CVE ID : CVE-2019-5868		
Use After Free	25-11-2019	4.3	Use after free in Blink in Google Chrome prior to 76.0.3809.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5869	N/A	A-GOO-CHRO-031219/35
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5870	N/A	A-GOO-CHRO-031219/36
Use After Free	25-11-2019	4.3	Use after free in Mojo in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5872	N/A	A-GOO-CHRO-031219/37
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5876	N/A	A-GOO-CHRO-031219/38
Use After Free	25-11-2019	6.8	Use after free in V8 in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to	N/A	A-GOO-CHRO-031219/39

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5878								
Use After Free	25-11-2019	6.8	Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13685	N/A	A-GOO-CHRO-031219/40						
Use After Free	25-11-2019	6.8	Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13686	N/A	A-GOO-CHRO-031219/41						
Use After Free	25-11-2019	6.8	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13687	N/A	A-GOO-CHRO-031219/42						
Use After Free	25-11-2019	6.8	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13688	N/A	A-GOO-CHRO-031219/43						
Use After Free	25-11-2019	6.8	Use after free in IndexedDB in Google Chrome prior to	N/A	A-GOO-CHRO-031219/44						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2019-13693		
Use After Free	25-11-2019	6.8	Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13694	N/A	A-GOO-CHRO-031219/45
Use After Free	25-11-2019	6.8	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13695	N/A	A-GOO-CHRO-031219/46
Use After Free	25-11-2019	6.8	Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13696	N/A	A-GOO-CHRO-031219/47
Use After Free	25-11-2019	6.8	Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted	N/A	A-GOO-CHRO-031219/48

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. CVE ID : CVE-2019-13699		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-11-2019	6.8	Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13700	N/A	A-GOO-CHRO-031219/49
Authentication Bypass by Spoofing	25-11-2019	4.3	Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. CVE ID : CVE-2019-13701	N/A	A-GOO-CHRO-031219/50
Improper Privilege Management	25-11-2019	6.8	Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable. CVE ID : CVE-2019-13702	N/A	A-GOO-CHRO-031219/51
Authentication Bypass by Spoofing	25-11-2019	4.3	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	N/A	A-GOO-CHRO-031219/52

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13703		
Authenticati on Bypass by Spoofing	25-11-2019	4.3	Insufficient policy enforcement in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass content security policy via a crafted HTML page. CVE ID : CVE-2019-13704	N/A	A-GOO-CHRO-031219/53
Information Exposure	25-11-2019	4.3	Insufficient policy enforcement in extensions in Google Chrome prior to 78.0.3904.70 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. CVE ID : CVE-2019-13705	N/A	A-GOO-CHRO-031219/54
Out-of- bounds Read	25-11-2019	6.8	Out of bounds memory access in PDFium in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2019-13706	N/A	A-GOO-CHRO-031219/55
Information Exposure	25-11-2019	4.3	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application. CVE ID : CVE-2019-13707	N/A	A-GOO-CHRO-031219/56
Authenticati on Bypass by	25-11-2019	4.3	Inappropriate implementation in	N/A	A-GOO-CHRO-031219/57

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Spoofing			navigation in Google Chrome on iOS prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. CVE ID : CVE-2019-13708		
Authentication Bypass by Spoofing	25-11-2019	4.3	Insufficient policy enforcement in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page. CVE ID : CVE-2019-13709	N/A	A-GOO-CHRO-031219/58
Improper Input Validation	25-11-2019	4.3	Insufficient validation of untrusted input in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page. CVE ID : CVE-2019-13710	N/A	A-GOO-CHRO-031219/59
Information Exposure	25-11-2019	5	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2019-13711	N/A	A-GOO-CHRO-031219/60
Information Exposure	25-11-2019	4.3	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a	N/A	A-GOO-CHRO-031219/61

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			crafted HTML page. CVE ID : CVE-2019-13713							
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	25-11-2019	4.3	Insufficient validation of untrusted input in Color Enhancer extension in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to inject CSS into an HTML page via a crafted URL. CVE ID : CVE-2019-13714	N/A	A-GOO-CHRO-031219/62					
Authentication Bypass by Spoofing	25-11-2019	4.3	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. CVE ID : CVE-2019-13715	N/A	A-GOO-CHRO-031219/63					
Insecure Storage of Sensitive Information	25-11-2019	4.3	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page. CVE ID : CVE-2019-13717	N/A	A-GOO-CHRO-031219/64					
Improper Input Validation	25-11-2019	4.3	Insufficient data validation in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name. CVE ID : CVE-2019-13718	N/A	A-GOO-CHRO-031219/65					
Insecure	25-11-2019	4.3	Incorrect security UI in full	N/A	A-GOO-CHRO-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page. CVE ID : CVE-2019-13719		031219/66
Use After Free	25-11-2019	6.8	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13720	N/A	A-GOO-CHRO-031219/67
Use After Free	25-11-2019	6.8	Use after free in PDFium in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-13721	N/A	A-GOO-CHRO-031219/68
Use After Free	25-11-2019	4.3	Use after free in Blink in Google Chrome prior to 75.0.3770.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5842	N/A	A-GOO-CHRO-031219/69
Use After Free	25-11-2019	6.8	Use after free in offline mode in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape	N/A	A-GOO-CHRO-031219/70

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			via a crafted HTML page. CVE ID : CVE-2019-5850							
Use After Free	25-11-2019	6.8	Use after free in WebAudio in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5851	N/A	A-GOO-CHRO-031219/71					
IBM										
security_identity_manager										
Deserializati on of Untrusted Data	20-11-2019	9.3	IBM Security Identity Manager 6.0.0 could allow a remote attacker to execute arbitrary code on the system, caused by the deserialization of untrusted data. By persuading a victim to visit a specially crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 166456. CVE ID : CVE-2019-4561	https://www.ibm.com/support/pages/node/1108695	A-IBM-SECU-031219/72					
maximo_asset_management										
Improper Authenticati on	20-11-2019	5.5	IBM Maximo Asset Management 7.6, 7.6.1, and 7.6.1.1 could allow an authenticated user to delete a record that they should not normally be able to. IBM X-Force ID: 165586. CVE ID : CVE-2019-4530	https://www.ibm.com/support/pages/node/1108503	A-IBM-MAXI-031219/73					
smartcloud_analytics_log_analysis										
Incorrect	22-11-2019	4.3	IBM SmartCloud Analytics	https://ww	A-IBM-SMAR-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authorization			1.3.1 through 1.3.5 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 159185. CVE ID : CVE-2019-4214	w.ibm.com/support/pages/node/1110171	031219/74					
Improper Input Validation	22-11-2019	4.3	IBM SmartCloud Analytics 1.3.1 through 1.3.5 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 159186. CVE ID : CVE-2019-4215	https://www.ibm.com/support/pages/node/1109769	A-IBM-SMAR-031219/75					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-11-2019	4.9	IBM SmartCloud Analytics 1.3.1 through 1.3.5 is vulnerable to possible host header injection attack that could lead to HTTP cache poisoning or firewall bypass. IBM X-Force ID: 159187. CVE ID : CVE-2019-4216	https://www.ibm.com/support/pages/node/1109745	A-IBM-SMAR-031219/76					
Information Exposure	22-11-2019	3.6	IBM SmartCloud Analytics 1.3.1 through 1.3.5 allows unauthorized disclosure of information like accessing solrconfig.xml and could allow an attacker to perform disruptive administrator	https://www.ibm.com/support/pages/node/1109721	A-IBM-SMAR-031219/77					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			tasks. IBM X-Force ID: 159517. CVE ID : CVE-2019-4243							
infoway										
social_photo_gallery										
Improper Input Validation	18-11-2019	4.6	The Social Photo Gallery plugin 1.0 for WordPress allows Remote Code Execution by creating an album and attaching a malicious PHP file in the cover photo album, because the file extension is not checked. CVE ID : CVE-2019-14467	N/A	A-INF-SOCI-031219/78					
iobroker										
iobroker.admin										
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-11-2019	7.5	iobroker.admin before 3.6.12 allows attacker to include file contents from outside the `/log/file1/` directory. CVE ID : CVE-2019-10765	N/A	A-IOB-IOBR-031219/79					
iterm2										
iterm2										
Information Exposure	17-11-2019	5	iTerm2 through 3.3.6 has potentially insufficient documentation about the presence of search history in com.googlecode.iterm2.plist, which might allow remote attackers to obtain sensitive information, as demonstrated by searching for the NoSyncSearchHistory string in .plist files within	N/A	A-ITE-ITER-031219/80					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			public Git repositories. CVE ID : CVE-2019-19022							
Jenkins										
support_core										
Improper Preservation of Permissions	21-11-2019	5.5	A missing permission check in Jenkins Support Core Plugin 2.63 and earlier allows attackers with Overall/Read permission to delete support bundles. CVE ID : CVE-2019-16539	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-1634	A-JEN-SUPP-031219/81					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-11-2019	5.5	A path traversal vulnerability in Jenkins Support Core Plugin 2.63 and earlier allows attackers with Overall/Read permission to delete arbitrary files on the Jenkins master. CVE ID : CVE-2019-16540	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-1634	A-JEN-SUPP-031219/82					
google_compute_engine										
Authorization Bypass Through User-Controlled Key	21-11-2019	4.3	Jenkins Google Compute Engine Plugin 4.1.1 and earlier does not verify SSH host keys when connecting agents created by the plugin, enabling man-in-the-middle attacks. CVE ID : CVE-2019-16546	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-1584	A-JEN-GOOG-031219/83					
Incorrect Permission Assignment for Critical Resource	21-11-2019	4	Missing permission checks in various API endpoints in Jenkins Google Compute Engine Plugin 4.1.1 and earlier allow attackers with Overall/Read permission to obtain limited information about the plugin configuration and	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-1585	A-JEN-GOOG-031219/84					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			environment. CVE ID : CVE-2019-16547							
Cross-Site Request Forgery (CSRF)	21-11-2019	6.8	A cross-site request forgery vulnerability in Jenkins Google Compute Engine Plugin 4.1.1 and earlier in ComputeEngineCloud#doProvision could be used to provision new agents. CVE ID : CVE-2019-16548	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-1586	A-JEN-GOOG-031219/85					
jhead_project										
jhead										
Out-of-bounds Read	17-11-2019	4.3	jhead 3.03 is affected by: heap-based buffer over-read. The impact is: Denial of service. The component is: ReadJpegSections and process_SOFn in jpgfile.c. The attack vector is: Open a specially crafted JPEG file. CVE ID : CVE-2019-19035	N/A	A-JHE-JHEA-031219/86					
kairosdb_project										
kairosdb										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-11-2019	4.3	KairosDB through 1.2.2 has XSS in view.html because of showMessage in js/graph.js, as demonstrated by view.html?q= with a '"sampling":{"value":"<script>' substring. CVE ID : CVE-2019-19040	N/A	A-KAI-KAIR-031219/87					
Lenovo										
customer_engagement_service										
Improper Privilege Management	20-11-2019	4.6	A potential vulnerability in the discontinued Customer Engagement Service (CCSDK) software version	N/A	A-LEN-CUST-031219/88					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.0.21.1 may allow local privilege escalation. CVE ID : CVE-2019-6184		
system_interface_foundation					
N/A	20-11-2019	6.5	A potential vulnerability was reported in Lenovo System Interface Foundation versions before v1.1.18.3 that could allow an authenticated user to execute code as another user. CVE ID : CVE-2019-6186	N/A	A-LEN-SYST-031219/89
Untrusted Search Path	20-11-2019	4.4	A potential vulnerability was reported in Lenovo System Interface Foundation versions before v1.1.18.3 that could allow an administrative user to load an unsigned DLL. CVE ID : CVE-2019-6189	N/A	A-LEN-SYST-031219/90
xclarity_controller					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.	N/A	A-LEN-XCLA-031219/91

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-6187							
paper										
Improper Privilege Management	20-11-2019	4.6	A potential vulnerability in the discontinued LenovoPaper software version 1.0.0.22 may allow local privilege escalation. CVE ID : CVE-2019-6191	N/A	A-LEN-PAPE-031219/92					
limnoria_project										
limnoria										
Improper Input Validation	16-11-2019	7.5	Eval injection in the Math plugin of Limnoria (before 2019.11.09) and Supybot (through 2018-05-09) allows remote unprivileged attackers to disclose information or possibly have unspecified other impact via the calc and icalc IRC commands. CVE ID : CVE-2019-19010	N/A	A-LIM-LIMN-031219/93					
Microfocus										
operations_agent										
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	4	XXE attack vulnerability on Micro Focus Operations Agent, affected version 12.0, 12.01, 12.02, 12.03, 12.04, 12.05, 12.06, 12.10, 12.11. The vulnerability could be exploited to do an XXE attack on Operations Agent. CVE ID : CVE-2019-17085	https://softwaresupport.softwaregrp.com/doc/KM03556426	A-MIC-OPER-031219/94					
Netapp										
ontap_select_deploy_administration_utility										
Improper Neutralization of Special	21-11-2019	7.5	ONTAP Select Deploy administration utility versions 2.11.2 through	https://security.netapp.com/advi	A-NET-ONTA-031219/95					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			2.12.2 are susceptible to a code injection vulnerability which when successfully exploited could allow an unauthenticated remote attacker to enable and use a privileged user account. CVE ID : CVE-2019-5509	sory/ntap-20191121-0001/	
Improper Input Validation	21-11-2019	6.5	All versions of ONTAP Select Deploy administration utility are susceptible to a vulnerability which when successfully exploited could allow an administrative user to escalate their privileges. CVE ID : CVE-2019-17272	https://security.netapp.com/advisory/ntap-20191121-0002/	A-NET-ONTA-031219/96
ngiflib_project					
ngiflib					
NULL Pointer Dereference	17-11-2019	5	MiniUPnP ngiflib 0.4 has a NULL pointer dereference in GifIndexToTrueColor in ngiflib.c via a file that lacks a palette. CVE ID : CVE-2019-19011	N/A	A-NGI-NGIF-031219/97
Nvidia					
gpumodeswitch					
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of	N/A	A-NVI-GPUM-031219/98

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			other devices not managed by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service. CVE ID : CVE-2019-5688		
nvflash					
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service. CVE ID : CVE-2019-5688	N/A	A-NVI-NVFL-031219/99
nvuflash					
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflsh32.sys, and nvflsh64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed	N/A	A-NVI-NVUF-031219/100

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service. CVE ID : CVE-2019-5688							
octopus										
server										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	3.5	A persistent cross-site scripting (XSS) vulnerability in Octopus Server 3.4.0 through 2019.10.5 allows remote authenticated attackers to inject arbitrary web script or HTML. CVE ID : CVE-2019-19085	N/A	A-OCT-SERV-031219/101					
octopus_deploy										
Unrestricted Upload of File with Dangerous Type	18-11-2019	4	In Octopus Deploy 3.3.0 through 2019.10.4, an authenticated user with PackagePush permission to upload packages could upload a maliciously crafted package, triggering an exception that exposes underlying operating system details. CVE ID : CVE-2019-19084	N/A	A-OCT-OCTO-031219/102					
oniguruma_project										
oniguruma										
Integer Overflow or Wraparound	17-11-2019	7.5	An integer overflow in the search_in_range function in regex.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version).	N/A	A-ONI-ONIG-031219/103					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Remote attackers can cause a denial-of-service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression. CVE ID : CVE-2019-19012							
openfind										
mail2000										
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-11-2019	4.3	The "/cgi-bin/go" page in MAIL2000 through version 6.0 and 7.0 has a cross-site scripting (XSS) vulnerability, allowing execution of arbitrary code via ACTION parameter without authentication. The code can be executed for any user accessing the page. This vulnerability affects many mail system of governments, organizations, companies and universities. CVE ID : CVE-2019-15071	https://gist.github.com/chtsecurity/21119b393640bea1d010ab9e3bee216d , https://gist.github.com/tonykuo76/95638395e0c83e68dbd3db0fa0184e27 , https://twntwcert.org.tw/taiwanvn/TVN-201909001 , https://www.openfind.com.tw/taiwan/resource.html	A-OPE-MAIL-031219/104					
Improper Neutralization of Input During Web Page Generation ('Cross-site	20-11-2019	4.3	The login feature in "/cgi-bin/portal" in MAIL2000 through version 6.0 and 7.0 has a cross-site scripting (XSS) vulnerability, allowing execution of arbitrary code via any parameter. This	https://gist.github.com/chtsecurity/b339650d4686ad47fb26f64967ef24a ,	A-OPE-MAIL-031219/105					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Scripting')			vulnerability affects many mail system of governments, organizations, companies and universities. CVE ID : CVE-2019-15072	https://gist.github.com/tonykuo76/5bf1ac369d953d5276afe0a2d04c2147 , https://tvn.twcert.org.tw/taiwanvn/TVN-201909002 , https://www.openfind.com.tw/taiwan/resource.html						
URL Redirection to Untrusted Site ('Open Redirect')	20-11-2019	5.8	An Open Redirect vulnerability for all browsers in MAIL2000 through version 6.0 and 7.0, which will redirect to a malicious site without authentication. This vulnerability affects many mail system of governments, organizations, companies and universities. CVE ID : CVE-2019-15073	https://gist.github.com/chtsecurity/512ebad24dddffb5321cf5f1a336f90f , https://gist.github.com/tonykuo76/ed1cc21cf755bfb8b67ca24f50bde13 , https://tvn.twcert.org.tw/taiwanvn/TVN-201909003 , https://www.openfind.com.tw/taiwan/resource.html	A-OPE-MAIL-031219/106					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
openwrt					
openwrt					
Improper Certificate Validation	18-11-2019	4.3	<p>An exploitable information leak vulnerability exists in the ustream-ssl library of OpenWrt, versions 18.06.4 and 15.05.1. When connecting to a remote server, the server's SSL certificate is checked but no action is taken when the certificate is invalid. An attacker could exploit this behavior by performing a man-in-the-middle attack, providing any certificate, leading to the theft of all the data sent by the client during the first request. After an SSL connection is initialized via <code>_ustream_ssl_init</code>, and after any data (e.g. the client's HTTP request) is written to the stream using <code>ustream_printf</code>, the code eventually enters the function <code>__ustream_ssl_poll</code>, which is used to dispatch the read/write events</p> <p>CVE ID : CVE-2019-5101</p>	N/A	A-OPE-OPEN-031219/107
Improper Certificate Validation	18-11-2019	4.3	<p>An exploitable information leak vulnerability exists in the ustream-ssl library of OpenWrt, versions 18.06.4 and 15.05.1. When connecting to a remote server, the server's SSL certificate is checked but no action is taken when the</p>	N/A	A-OPE-OPEN-031219/108

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			certificate is invalid. An attacker could exploit this behavior by performing a man-in-the-middle attack, providing any certificate, leading to the theft of all the data sent by the client during the first request. CVE ID : CVE-2019-5102							
Pimcore										
pimcore										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-11-2019	4	pimcore/pimcore before 6.3.0 is vulnerable to SQL Injection. An attacker with limited privileges (classes permission) can achieve a SQL injection that can lead in data leakage. The vulnerability can be exploited via 'id', 'storeId', 'pageSize' and 'tables' parameters, using a payload for trigger a time based or error based sql injection. CVE ID : CVE-2019-10763	N/A	A-PIM-PIMC-031219/109					
pixie_project										
pixie										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-11-2019	7.5	Pixie versions 1.0.x before 1.0.3, and 2.0.x before 2.0.2 allow SQL Injection in the limit() function due to improper sanitization. CVE ID : CVE-2019-10766	N/A	A-PIX-PIXI-031219/110					
Postgresql										
postgresql-common										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	20-11-2019	7.2	The pg_ctlcluster script in postgresql-common in versions prior to 210 didn't drop privileges when creating socket/statistics temporary directories, which could result in local privilege escalation. CVE ID : CVE-2019-3466	N/A	A-POS-POST-031219/111
qmetry					
jenkins_qmetry_for_jira					
Insufficiently Protected Credentials	21-11-2019	4	Jenkins QMetry for JIRA - Test Management Plugin 1.12 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-16544	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-727%20(1)	A-QME-JENK-031219/112
Insufficiently Protected Credentials	21-11-2019	4	Jenkins QMetry for JIRA - Test Management Plugin transmits credentials in its configuration in plain text as part of job configuration forms, potentially resulting in their exposure. CVE ID : CVE-2019-16545	https://jenkins.io/security/advisory/2019-11-21/#SECURITY-727%20(2)	A-QME-JENK-031219/113
Qualcomm					
ips					
Integer Overflow or Wraparound	21-11-2019	7.5	Integer overflow to buffer overflow vulnerability in PostScript image handling code used by the PostScript- and PDF-compatible interpreters due to incorrect	https://www.qualcomm.com/company/product-security/bu	A-QUA-IPS-031219/114

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			buffer size calculation. in PostScript and PDF printers that use IPS versions prior to 2019.2 in PostScript and PDF printers that use IPS versions prior to 2019.2 CVE ID : CVE-2019-10627	lletins/october-2019-bulletin						
rconfig										
rconfig										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-11-2019	6.5	rConfig 3.9.2 allows devices.php?searchColumn=SQL injection. CVE ID : CVE-2019-19207	N/A	A-RCO-RCON-031219/115					
Redhat										
jboss_fuse										
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-asl libraries but in different classes. CVE ID : CVE-2019-10172	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10172	A-RED-JBOS-031219/116					
jboss_enterprise_application_platform										
Improper Restriction of XML External Entity Reference ('XXE')	18-11-2019	5	A flaw was found in org.codehaus.jackson:jackson-mapper-asl:1.9.x libraries. XML external entity vulnerabilities similar CVE-2016-3720 also affects codehaus jackson-mapper-	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10172	A-RED-JBOS-031219/117					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			asl libraries but in different classes. CVE ID : CVE-2019-10172							
Redmine										
redmine										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-11-2019	4	A SQL injection vulnerability in Redmine through 3.2.9 and 3.3.x before 3.3.10 allows Redmine users to access protected information via a crafted object query. CVE ID : CVE-2019-18890	N/A	A-RED-REDM-031219/118					
sandline										
centraleyezer										
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	Sandline Centraleyezer (On Premises) allows unrestricted File Upload with a dangerous type, because the feature of adding ".jpg" to any uploaded filename is not enforced on the server side. CVE ID : CVE-2019-12271	N/A	A-SAN-CENT-031219/119					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-11-2019	4.3	Sandline Centraleyezer (On Premises) allows Stored XSS using HTML entities in the name field of the Category section. CVE ID : CVE-2019-12299	N/A	A-SAN-CENT-031219/120					
Improper Neutralization of Input During Web Page	18-11-2019	4.3	Sandline Centraleyezer (On Premises) allows Unrestricted File Upload leading to Stored XSS. An HTML page running a script	N/A	A-SAN-CENT-031219/121					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			could be uploaded to the server. When a victim tries to download a CISO Report template, the script is loaded. CVE ID : CVE-2019-12311		
simplito					
elliptic-php					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-11-2019	5.8	In elliptic-php versions prior to 1.0.6, Timing attacks might be possible which can result in practical recovery of the long-term private key generated by the library under certain conditions. Leakage of a bit-length of the scalar during scalar multiplication is possible on an elliptic curve which might allow practical recovery of the long-term private key. CVE ID : CVE-2019-10764	N/A	A-SIM-ELLI-031219/122
Symantec					
norton_app_lock					
N/A	18-11-2019	4.4	Norton App Lock, prior to 1.4.0.503, may be susceptible to a bypass exploit. In this type of circumstance, the exploit can allow the user to circumvent the app to prevent it from locking other apps on the device, thereby allowing the individual to gain access. CVE ID : CVE-2019-18373	https://support.symantec.com/us/en/article.SYMSA1496.html	A-SYM-NORT-031219/123
Vmware					
workstation					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process. CVE ID : CVE-2019-5540	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-WORK-031219/124
Out-of-bounds Write	20-11-2019	6.5	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM. CVE ID : CVE-2019-5541	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-WORK-031219/125
Improper Input Validation	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain a denial-of-service vulnerability in the RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. CVE ID : CVE-2019-5542	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-WORK-031219/126

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fusion					
Information Exposure	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process. CVE ID : CVE-2019-5540	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-FUSI-031219/127
Out-of-bounds Write	20-11-2019	6.5	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM. CVE ID : CVE-2019-5541	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-FUSI-031219/128
Improper Input Validation	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain a denial-of-service vulnerability in the RPC handler. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM.	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	A-VMW-FUSI-031219/129

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5542		
xorur					
lpar2rrd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control) and injecting malicious code into the upgrade.sh file. CVE ID : CVE-2019-19041	N/A	A-XOR-LPAR-031219/130
stor2rrd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control)	N/A	A-XOR-STOR-031219/131

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and injecting malicious code into the upgrade.sh file. CVE ID : CVE-2019-19041		
xorur					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-11-2019	9	An issue was discovered in Xorux Lpar2RRD 6.11 and Stor2RRD 2.61, as distributed in Xorux 2.41. They do not correctly verify the integrity of an upgrade package before processing it. As a result, official upgrade packages can be modified to inject an arbitrary Bash script that will be executed by the underlying system. It is possible to achieve this by modifying the values in the files.SUM file (which are used for integrity control) and injecting malicious code into the upgrade.sh file. CVE ID : CVE-2019-19041	N/A	A-XOR-XORU-031219/132
Operating System					
Apple					
mac_os_x					
Information Exposure	20-11-2019	4	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an information disclosure vulnerability in vmnetdhcp. Successful exploitation of this issue may allow an attacker on a guest VM to disclose sensitive information by leaking memory from the host process.	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	O-APP-MAC_-031219/133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-5540							
Out-of-bounds Write	20-11-2019	6.5	VMware Workstation (15.x before 15.5.1) and Fusion (11.x before 11.5.1) contain an out-of-bounds write vulnerability in the e1000e virtual network adapter. Successful exploitation of this issue may lead to code execution on the host from the guest or may allow attackers to create a denial-of-service condition on their own VM. CVE ID : CVE-2019-5541	https://www.vmware.com/security/advisories/VMSA-2019-0021.html	O-APP-MAC_-031219/134					
Canonical										
ubuntu_linux										
Improper Privilege Management	20-11-2019	7.2	The pg_ctlcluster script in postgresql-common in versions prior to 210 didn't drop privileges when creating socket/statistics temporary directories, which could result in local privilege escalation. CVE ID : CVE-2019-3466	N/A	O-CAN-UBUN-031219/135					
Debian										
debian_linux										
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-11-2019	4	A SQL injection vulnerability in Redmine through 3.2.9 and 3.3.x before 3.3.10 allows Redmine users to access protected information via a crafted object query. CVE ID : CVE-2019-18890	N/A	O-DEB-DEBI-031219/136					
Improper	20-11-2019	7.2	The pg_ctlcluster script in	N/A	O-DEB-DEBI-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			postgresql-common in versions prior to 210 didn't drop privileges when creating socket/statistics temporary directories, which could result in local privilege escalation. CVE ID : CVE-2019-3466		031219/137
Fedoraproject					
fedora					
Improper Input Validation	16-11-2019	7.5	Eval injection in the Math plugin of Limnoria (before 2019.11.09) and Supybot (through 2018-05-09) allows remote unprivileged attackers to disclose information or possibly have unspecified other impact via the calc and icalc IRC commands. CVE ID : CVE-2019-19010	N/A	O-FED-FEDO-031219/138
Fortinet					
fortios					
Use of Hard-coded Credentials	21-11-2019	4	Use of a hard-coded cryptographic key to cipher sensitive data in FortiOS configuration backup file may allow an attacker with access to the backup file to decipher the sensitive data, via knowledge of the hard-coded key. The aforementioned sensitive data includes users' passwords (except the administrator's password), private keys' passphrases and High Availability	https://fortiguard.com/advisory/FG-IR-19-007	O-FOR-FORT-031219/139

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			password (when set). CVE ID : CVE-2019-6693							
Lenovo										
thinkpad_usb-c_dock_firmware										
N/A	20-11-2019	5	A potential vulnerability reported in ThinkPad USB-C Dock Firmware version 3.7.2 may allow a denial of service. CVE ID : CVE-2019-6176	N/A	O-LEN-THIN-031219/140					
Linksys										
velop_whw0303_firmware										
Authorization Bypass Through User-Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340	N/A	O-LIN-VELO-031219/141					
velop_whw0302_firmware										
Authorization Bypass Through User-Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340	N/A	O-LIN-VELO-031219/142					
velop_whw0301_firmware										
Authorization Bypass Through User-Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340	N/A	O-LIN-VELO-031219/143					
Linux										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
linux_kernel										
Unrestricted Upload of File with Dangerous Type	18-11-2019	7.5	The 8.1.1 and 8.2.0 releases of Apache Solr contain an insecure setting for the ENABLE_REMOTE_JMX_OPTS configuration option in the default solr.in.sh configuration file shipping with Solr. If you use the default solr.in.sh file from the affected releases, then JMX monitoring will be enabled and exposed on RMI_PORT (default=18983), without any authentication. If this port is opened for inbound traffic in your firewall, then anyone with network access to your Solr nodes will be able to access JMX, which may in turn allow them to upload malicious code for execution on the Solr server. CVE ID : CVE-2019-12409	N/A	O-LIN-LINU-031219/144					
NULL Pointer Dereference	21-11-2019	4.3	btrfs_root_node in fs/btrfs/ctree.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because rcu_dereference(root->node) can be zero. CVE ID : CVE-2019-19036	N/A	O-LIN-LINU-031219/145					
NULL Pointer Dereference	21-11-2019	4.3	ext4_empty_dir in fs/ext4/namei.c in the Linux kernel through 5.3.12 allows a NULL pointer dereference because ext4_read_dirblock(inode,0, DIRENT_HTREE) can be	N/A	O-LIN-LINU-031219/146					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zero. CVE ID : CVE-2019-19037		
Information Exposure	21-11-2019	1.9	__btrfs_free_extent in fs/btrfs/extent-tree.c in the Linux kernel through 5.3.12 calls btrfs_print_leaf in a certain ENOENT case, which allows local users to obtain potentially sensitive information about register values via the dmesg program. CVE ID : CVE-2019-19039	N/A	O-LIN-LINU-031219/147
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the i40e_setup_macvlans() function in drivers/net/ethernet/intel/i40e/i40e_main.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering i40e_setup_channel() failures, aka CID-27d461333459. CVE ID : CVE-2019-19043	N/A	O-LIN-LINU-031219/148
Uncontrolled Resource Consumption	18-11-2019	7.8	Two memory leaks in the v3d_submit_cl_ioctl() function in drivers/gpu/drm/v3d/v3d_gem.c in the Linux kernel before 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering kcalloc() or v3d_job_init() failures, aka CID-29cd13cfd762. CVE ID : CVE-2019-19044	N/A	O-LIN-LINU-031219/149

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the <code>mlx5_fpga_conn_create_cq()</code> function in <code>drivers/net/ethernet/mellanox/mlx5/core/fpga/conn.c</code> in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering <code>mlx5_vector2eqn()</code> failures, aka CID-c8c2a057fdc7. CVE ID : CVE-2019-19045	N/A	O-LIN-LINU-031219/150
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the <code>__ipmi_bmc_register()</code> function in <code>drivers/char/ipmi/ipmi_msg_handler.c</code> in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering <code>ida_simple_get()</code> failure, aka CID-4aa7afb0ee20. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control this failure at probe time. CVE ID : CVE-2019-19046	N/A	O-LIN-LINU-031219/151
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the <code>mlx5_fw_fatal_reporter_dump()</code> function in <code>drivers/net/ethernet/mellanox/mlx5/core/health.c</code> in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by	N/A	O-LIN-LINU-031219/152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			triggering mlx5_crump_collect() failures, aka CID- c7ed6d0183d5. CVE ID : CVE-2019-19047		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_reportstat() function in drivers/virt/vboxguest/vbo xguest_utils.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering copy_form_user() failures, aka CID-e0b0cb938864. CVE ID : CVE-2019-19048	N/A	O-LIN-LINU- 031219/153
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the unittest_data_add() function in drivers/of/unittest.c in the Linux kernel before 5.3.10 allows attackers to cause a denial of service (memory consumption) by triggering of_fdt_unflatten_tree() failures, aka CID- e13de8fe0d6a. NOTE: third parties dispute the relevance of this because unittest.c can only be reached during boot. CVE ID : CVE-2019-19049	N/A	O-LIN-LINU- 031219/154
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_reportstat() function in crypto/crypto_user_stat.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service	N/A	O-LIN-LINU- 031219/155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(memory consumption) by triggering crypto_reportstat_alg() failures, aka CID-c03b04dcdba1. CVE ID : CVE-2019-19050		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the i2400m_op_rfkill_sw_toggle() function in drivers/net/wimax/i2400m/op-rfkill.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-6f3ef5c25cc7. CVE ID : CVE-2019-19051	N/A	O-LIN-LINU-031219/156
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the gs_can_open() function in drivers/net/can/usb/gs_usb.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-fb5be6a7b486. CVE ID : CVE-2019-19052	N/A	O-LIN-LINU-031219/157
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rpmsg_eptdev_write_iter() function in drivers/rpmsg/rpmsg_char.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy_from_iter_full() failures, aka CID-	N/A	O-LIN-LINU-031219/158

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bbe692e349e2. CVE ID : CVE-2019-19053		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885/cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b. CVE ID : CVE-2019-19054	N/A	O-LIN-LINU-031219/159
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the nl80211_get_ftm_responder_stats() function in net/wireless/nl80211.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering nl80211hdr_put() failures, aka CID-1399c59fa929. NOTE: third parties dispute the relevance of this because it occurs on a code path where a successful allocation has already occurred. CVE ID : CVE-2019-19055	N/A	O-LIN-LINU-031219/160
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the mwifiex_pcie_alloc_cmdrsp_buf() function in drivers/net/wireless/marvell/mwifiex/pcie.c in the Linux kernel through 5.3.11 allows attackers to cause a	N/A	O-LIN-LINU-031219/161

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-db8fd2cde932. CVE ID : CVE-2019-19056		
Uncontrolled Resource Consumption	18-11-2019	7.8	Two memory leaks in the mwifiex_pcie_init_evt_ring() function in drivers/net/wireless/marvell/mwifiex/pcie.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering mwifiex_map_pci_memory() failures, aka CID-d10dcb615c8e. CVE ID : CVE-2019-19057	N/A	O-LIN-LINU-031219/162
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the alloc_sgtable() function in drivers/net/wireless/intel/iwlwifi/fw/dbg.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering alloc_page() failures, aka CID-b4b814fec1a5. CVE ID : CVE-2019-19058	N/A	O-LIN-LINU-031219/163
Uncontrolled Resource Consumption	18-11-2019	7.8	Multiple memory leaks in the iwl_pcie_ctxt_info_gen3_init() function in drivers/net/wireless/intel/iwlwifi/pcie/ctxt-info-gen3.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service	N/A	O-LIN-LINU-031219/164

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(memory consumption) by triggering iwl_pcie_init_fw_sec() or dma_alloc_coherent() failures, aka CID- 0f4f199443fa. CVE ID : CVE-2019-19059		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the adis_update_scan_mode() function in drivers/iio/imu/adis_buffer. c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-ab612b1daf41. CVE ID : CVE-2019-19060	N/A	O-LIN-LINU- 031219/165
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the adis_update_scan_mode_bur st() function in drivers/iio/imu/adis_buffer. c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-9c0530e898f3. CVE ID : CVE-2019-19061	N/A	O-LIN-LINU- 031219/166
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the crypto_report() function in crypto/crypto_user_base.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering crypto_report_alg() failures, aka CID-ffdde5932042. CVE ID : CVE-2019-19062	N/A	O-LIN-LINU- 031219/167

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	18-11-2019	7.8	Two memory leaks in the rtl_usb_probe() function in drivers/net/wireless/realtek/rtlwifi/usb.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption), aka CID-3f9361695113. CVE ID : CVE-2019-19063	N/A	O-LIN-LINU-031219/168
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the fsl_lpspi_probe() function in drivers/spi/spi-fsl-lpspi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering pm_runtime_get_sync() failures, aka CID-057b8945f78f. NOTE: third parties dispute the relevance of this because an attacker cannot realistically control these failures at probe time. CVE ID : CVE-2019-19064	N/A	O-LIN-LINU-031219/169
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the sdma_init() function in drivers/infiniband/hw/hfi1/sdma.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering rhashtable_init() failures, aka CID-34b3be18a04e. CVE ID : CVE-2019-19065	N/A	O-LIN-LINU-031219/170
Uncontrolled Resource	18-11-2019	7.8	A memory leak in the bfad_im_get_stats() function	N/A	O-LIN-LINU-031219/171

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Consumption			in drivers/scsi/bfa/bfad_attr.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering bfa_port_get_stats() failures, aka CID-0e62395da2bd. CVE ID : CVE-2019-19066							
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** Four memory leaks in the acp_hw_init() function in drivers/gpu/drm/amd/amdgpu/amdgpu_acp.c in the Linux kernel before 5.3.8 allow attackers to cause a denial of service (memory consumption) by triggering mfd_add_hotplug_devices() or pm_genpd_add_device() failures, aka CID-57be09c6e874. NOTE: third parties dispute the relevance of this because the attacker must already have privileges for module loading. CVE ID : CVE-2019-19067	N/A	O-LIN-LINU-031219/172					
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rtl8xxxu_submit_int_urb() function in drivers/net/wireless/realtek/rtl8xxxu/rtl8xxxu_core.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-a2cdd07488e6.	N/A	O-LIN-LINU-031219/173					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-19068							
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the fastrpc_dma_buf_attach() function in drivers/misc/fastrpc.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering dma_get_sgtable() failures, aka CID-fc739a058d99. CVE ID : CVE-2019-19069	N/A	O-LIN-LINU-031219/174					
Uncontrolled Resource Consumption	18-11-2019	7.8	** DISPUTED ** A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering devm_add_action_or_reset() failures, aka CID-d3b0ffa1d75d. NOTE: third parties dispute the relevance of this because the system must have already been out of memory before the probe began. CVE ID : CVE-2019-19070	N/A	O-LIN-LINU-031219/175					
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the rsi_send_beacon() function in drivers/net/wireless/rsi/rsi_91x_mgmt.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering rsi_prepare_beacon() failures, aka CID-	N/A	O-LIN-LINU-031219/176					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			d563131ef23c. CVE ID : CVE-2019-19071		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the predicate_parse() function in kernel/trace/trace_events_filter.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-96c5c6e6a5b6. CVE ID : CVE-2019-19072	N/A	O-LIN-LINU-031219/177
Uncontrolled Resource Consumption	18-11-2019	7.8	Memory leaks in drivers/net/wireless/ath/ath9k/htc_hst.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering wait_for_completion_timeout() failures. This affects the htc_config_pipe_credits() function, the htc_setup_complete() function, and the htc_connect_service() function, aka CID-853acf7caf10. CVE ID : CVE-2019-19073	N/A	O-LIN-LINU-031219/178
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/ath9k/wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728c1e2a05e4.	N/A	O-LIN-LINU-031219/179

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			CVE ID : CVE-2019-19074								
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ca8210_probe() function in drivers/net/ieee802154/ca8210.c in the Linux kernel before 5.3.8 allows attackers to cause a denial of service (memory consumption) by triggering ca8210_get_platform_data() failures, aka CID-6402939ec86e. CVE ID : CVE-2019-19075	N/A	O-LIN-LINU-031219/180						
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the nfp_abm_u32_knode_replace() function in drivers/net/ethernet/netronome/nfp/abm/cls.c in the Linux kernel before 5.3.6 allows attackers to cause a denial of service (memory consumption), aka CID-78beef629fd9. CVE ID : CVE-2019-19076	N/A	O-LIN-LINU-031219/181						
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the bnxt_re_create_srq() function in drivers/infiniband/hw/bnxt_re/ib_verbs.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering copy to udata failures, aka CID-4a9d46a9fe14. CVE ID : CVE-2019-19077	N/A	O-LIN-LINU-031219/182						
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the ath10k_usb_hif_tx_sg() function in	N/A	O-LIN-LINU-031219/183						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			drivers/net/wireless/ath/at h10k/usb.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-b8d17e7d93d2. CVE ID : CVE-2019-19078		
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the qrtr_tun_write_iter() function in net/qrtr/tun.c in the Linux kernel before 5.3 allows attackers to cause a denial of service (memory consumption), aka CID- a21b7f0cff19. CVE ID : CVE-2019-19079	N/A	O-LIN-LINU- 031219/184
Uncontrolled Resource Consumption	18-11-2019	7.8	Four memory leaks in the nfp_flower_spawn_phy_reprs () function in drivers/net/ethernet/netro nome/nfp/flower/main.c in the Linux kernel before 5.3.4 allow attackers to cause a denial of service (memory consumption), aka CID- 8572cea1461a. CVE ID : CVE-2019-19080	N/A	O-LIN-LINU- 031219/185
Uncontrolled Resource Consumption	18-11-2019	7.8	A memory leak in the nfp_flower_spawn_vnic_repr s() function in drivers/net/ethernet/netro nome/nfp/flower/main.c in the Linux kernel before 5.3.4 allows attackers to cause a denial of service (memory consumption), aka CID- 8ce39eb5a67a.	N/A	O-LIN-LINU- 031219/186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-19081		
Uncontrolled Resource Consumption	18-11-2019	7.8	<p>Memory leaks in *create_resource_pool() functions under drivers/gpu/drm/amd/display/dc in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption). This affects the dce120_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce120/dce120_resource.c, the dce110_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce110/dce110_resource.c, the dce100_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce100/dce100_resource.c, the dcn10_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dcn10/dcn10_resource.c, and the dce112_create_resource_pool() function in drivers/gpu/drm/amd/display/dc/dce112/dce112_resource.c, aka CID-104c307147ad.</p> <p>CVE ID : CVE-2019-19082</p>	N/A	O-LIN-LINU-031219/187
Uncontrolled Resource	18-11-2019	7.8	Memory leaks in *clock_source_create()	N/A	O-LIN-LINU-031219/188

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			<p>functions under drivers/gpu/drm/amd/display/dc in the Linux kernel before 5.3.8 allow attackers to cause a denial of service (memory consumption). This affects the dce112_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce112/dce112_resource.c, the dce100_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce100/dce100_resource.c, the dcn10_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dcn10/dcn10_resource.c, the dcn20_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dcn20/dcn20_resource.c, the dce120_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce120/dce120_resource.c, the dce110_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce110/dce110_resource.c, and the dce80_clock_source_create() function in drivers/gpu/drm/amd/display/dc/dce80/dce80_resource.c.</p>		

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			e.c, aka CID-055e547478a1. CVE ID : CVE-2019-19083		
Microsoft					
windows					
Untrusted Search Path	19-11-2019	6.9	Code42 app through version 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a non-administrative attacker on the local machine could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local machine. CVE ID : CVE-2019-16860	https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_security_advisories/Arbitrary_code_execution_on_local_Windows_devices	O-MIC-WIND-031219/189
Untrusted Search Path	19-11-2019	6.9	Code42 server through 7.0.2 for Windows has an Untrusted Search Path. In certain situations, a non-administrative attacker on the local server could create or modify a dynamic-link library (DLL). The Code42 service could then load it at runtime, and potentially execute arbitrary code at an elevated privilege on the local server. CVE ID : CVE-2019-16861	https://code42.com/r/support/CVE-2019-16861	O-MIC-WIND-031219/190
Improper Privilege Management	18-11-2019	7.2	NVIDIA NVFlash, NVUFlash Tool prior to v5.588.0 and GPUModeSwitch Tool prior to 2019-11, NVIDIA kernel mode driver (nvflash.sys, nvflash32.sys, and	N/A	O-MIC-WIND-031219/191

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			nvflash64.sys) contains a vulnerability in which authenticated users with administrative privileges can gain access to device memory and registers of other devices not managed by NVIDIA, which may lead to escalation of privileges, information disclosure, or denial of service. CVE ID : CVE-2019-5688							
phicomm										
k2\((psg1218\)_firmware										
Improper Input Validation	18-11-2019	9	/usr/lib/lua/luci/controller/admin/autoupgrade.lua on PHICOMM K2(PSG1218) V22.5.9.163 devices allows remote authenticated users to execute any command via shell metacharacters in the cgi-bin/luci autoUpTime parameter. CVE ID : CVE-2019-19117	N/A	O-PHI-K2\(-031219/192					
Qualcomm										
qca6574au_firmware										
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA6-031219/193					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA6-031219/194
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA6-031219/195

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	bulletin	
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA6-031219/196

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8150 CVE ID : CVE-2019-2297							
qcs405_firmware										
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/197					
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octo	O-QUA-QCS4-031219/198					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	ber-2019-bulletin						
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/199					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/200					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/201

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/202
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/203

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/204					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/205					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150</p> <p>CVE ID : CVE-2019-2297</p>	security/bulletins/october-2019-bulletin	

ipq4019_firmware

Use After Free	21-11-2019	4.6	<p>Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ4-031219/206
----------------	------------	-----	---	---	-----------------------

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266							
Integer Underflow (Wrap or Wraparound)		21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-IPQ4-031219/207
ipq8064_firmware											
Use After Free		21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon					https://www.qualcomm.com/company/product-security/bulletins/october-2019-		O-QUA-IPQ8-031219/208
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	bulletin	
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ8-031219/209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8074_firmware					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ8-031219/210
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-IPQ8-031219/211

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318							
qca6174a_firmware										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA6-031219/212					
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN	https://www.qualcomm.com/com	O-QUA-QCA6-031219/213					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non- standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-QCA6- 031219/214					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
qca9377_firmware										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/215					
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-QCA9-031219/216					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	bulletin	
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/217

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8150 CVE ID : CVE-2019-2297							
qca9379_firmware										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/218					
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/219					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/220
apq8009_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/221					
Time-of-check Time-of-use (TOCTOU) Race	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/222					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Condition			bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/223					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/224					
Out-of-	21-11-2019	7.5	Possible OOB read issue in	https://ww	O-QUA-APQ8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/225					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/226					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/227					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/228					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
				SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Integer Underflow (Wrap or Wraparound)		21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/229	
Out-of-bounds Read		21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/230	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303								
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/231
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

apq8098_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/232
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/233					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
				QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free		21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/234	
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of				https://www.qualcomm.com/com		O-QUA-APQ8-031219/235	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/236

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20 CVE ID : CVE-2019-10535		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/237
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/239					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/240					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/242					
msm8939_firmware										
Time-of-check Time-of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://www.qualcomm.com/	O-QUA-MSM8-031219/243					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
(TOCTOU) Race Condition			modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/244					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/245					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/246					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/247					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
msm8953_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/248

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/249
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-MSM8-031219/250

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/251					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/252					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/253

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/254
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/255

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/256
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/257					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		
msm8998_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/258

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/259					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/260					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/261					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/262					
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/263					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	<p>If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2251</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/264
Out-of-bounds Read	21-11-2019	7.5	<p>Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/266					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/267					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/268
Out-of-bounds Read	21-11-2019	7.5	SNDTCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/269

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	ber-2019-bulletin						
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/270					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

nicobar_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/271
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/272					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/273					
Buffer Copy	21-11-2019	4.6	Buffer overflow can occur in	https://ww	O-QUA-NICO-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
without Checking Size of Input ('Classic Buffer Overflow')			wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/274					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/275					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/276
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/277

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/278					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer		21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/279
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-NICO-031219/280					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		

apq8053_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/281
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/282
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/283

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490						security/bulletins/october-2019-bulletin		
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/284
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/285
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/287
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/288

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	bulletin	
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/289
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/290

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	ct-security/bulletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octo	O-QUA-APQ8-031219/291					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ber-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/292					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/293					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/294

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	<p>While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2315</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/295
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	ct-security/bulletins/october-2019-bulletin	

mdm9207c_firmware

Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/297
---	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/299					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/300					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/301
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/302

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/303

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8905_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	<p>While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2335</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/304
Time-of-check Time-of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://www.qualcomm.com/	O-QUA-MSM8-031219/305

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
(TOCTOU) Race Condition			modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA- MSM8- 031219/306					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/307

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10503		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/308
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/310					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer		21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/311
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/312
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/313

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					ct-security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-		O-QUA-MSM8-031219/314
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	bulletin	

qcn7605_firmware

Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/315
---	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/317
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/318

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/319
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCN7-031219/320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		

sdm845_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/321
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/322
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/323

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/324					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/326

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/327					
Use After	21-11-2019	4.6	Possible double free issue in	https://ww	O-QUA-SDM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Free			kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/328					
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDM8- 031219/329					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/331					
Improper Restriction of	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG	https://www.qualcomm.com/	O-QUA-SDM8-031219/332					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Operations within the Bounds of a Memory Buffer			buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	pany/produ ct-security/bulletins/october-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/333					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/334					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/335

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/336					
apq8017_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/337					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/338					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/339
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/340

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	lletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/341					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/342
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/343

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/344					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/345					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/346
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/347

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	ct-security/bulletins/october-2019-bulletin						
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-APQ8-031219/348					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315						bulletin		
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-APQ8-031219/349
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		

apq8096au_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/350
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/351
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	security/bulletins/october-2019-bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/353					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/354
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/355

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/356
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/357

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	bulletin	
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/358

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2271</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/359
Improper	21-11-2019	10	Lack of integrity check	https://www	O-QUA-APQ8-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authentication			allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/360					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/361					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
)			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/362					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/363					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/364					
msm8976_firmware										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/365					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Infinite Loop')			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-MSM8-031219/366					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/367					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/368					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

sda845_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/369
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/370
Time-of-check Time-of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
(TOCTOU) Race Condition			modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/372					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/373
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/374

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/375					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/376					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/377

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/378
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/379

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/380					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/381					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA8-031219/382					
sdm636_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/383					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition		21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SDM6-031219/384
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/385
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/386

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	ber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/387
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN	https://www.qualcomm.com/	O-QUA-SDM6-031219/388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	pany/produ ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/389					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/390					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/391					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/392
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/393

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/394					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

sdm670_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/395
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/396
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/397

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490						security/bulletins/october-2019-bulletin		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SDM6-031219/398
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/399
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/401					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/402					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/403

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2295		
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/404
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,	https://www.qualcomm.com/com	O-QUA-SDM6-031219/405

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315					pany/produ ct- security/bu lletins/octo ber-2019- bulletin		
Use After Free		21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired					https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-		O-QUA-SDM6-031219/406
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	bulletin	
sdm710_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/407

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/408
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/409

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/410					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/411
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/412

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/413
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/414

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	ct-security/bulletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/415					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ber-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/416					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/417					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch	NCIIPC ID	
				MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/418	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM7-031219/419					
sm6150_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/420					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/421					
Improper Restriction	21-11-2019	7.2	Out of bound access due to lack of check of whitelist	https://www.qualcomm.com	O-QUA-SM61-031219/422					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
of Operations within the Bounds of a Memory Buffer			array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	m.com/company/product-security/bulletins/october-2019-bulletin						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/423					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/424
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/425

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/426					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/427
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/429					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/430					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/431					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM61-031219/432					
qm215_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QM21-031219/433					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QM21-031219/434					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QM21-031219/435					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QM21-031219/436					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QM21-031219/437					
Out-of-bounds Read	21-11-2019	7.5	SNDACP module may access array out side its boundary	https://www.qualcomm.com	O-QUA-QM21-031219/438					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	m.com/company/product-security/bulletins/october-2019-bulletin						
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octo	O-QUA-QM21-031219/439					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315						ber-2019-bulletin		
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-QM21-031219/440
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		
qca8081_firmware					
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA8-031219/441
qcs404_firmware					
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/442

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	ct-security/bulletins/october-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/443					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/444					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295						bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-QCS4-031219/445
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS4-031219/446					
sm8150_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-SM81-031219/447					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335					bulletin		
Use After Free		21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SM81-031219/448
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/449
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/451					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/453

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/454
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/455

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	lletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-SM81-031219/456					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289					bulletin		
Integer Underflow (Wrap or Wraparound)		21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SM81-031219/457
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/458					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/459					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM81-031219/460					
mdm9206_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/461					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/462					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/463
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/464

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503					ct-security/bulletins/october-2019-bulletin		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/465
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/466
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/467

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/468					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/469					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/470
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/471

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/472
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		

mdm9607_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/473
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/474					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/475
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/477					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/478
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/479

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/480					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/481					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/482
Out-of-bounds Read	21-11-2019	7.5	SNDTCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/483

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/484
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

mdm9650_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/485
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/486					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/487
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/488

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/489					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/490
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/491

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/492					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/493					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/494					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/495					
mdm9655_firmware										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/496					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/497					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	security/bulletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-MDM9-031219/498					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289					bulletin		
Out-of-bounds Read		21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/499
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
msm8996au_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/501					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/502

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	<p>Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20</p> <p>CVE ID : CVE-2019-10503</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/503
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	<p>Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/505
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/506

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/507
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/509					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/510					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/511					
Out-of-	21-11-2019	7.5	SNDCP module may access	https://ww	O-QUA-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	MSM8- 031219/512					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon	https://ww w.qualcom m.com/com pany/produ ct- security/bu	O-QUA- MSM8- 031219/513					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date		CVSS		Description & CVE ID				Patch		NCIIPC ID									
						Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315				lletins/october-2019-bulletin											
Out-of-bounds Read		21-11-2019		2.1		Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MSM8-031219/514									
CV Scoring Scale (CVSS)		0-1		1-2		2-3		3-4		4-5		5-6		6-7		7-8		8-9		9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		

mdm9615_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/515
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/516					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/517					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/518
mdm9625_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/519					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/520					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	security/bulletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-MDM9-031219/521					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289					bulletin		
Out-of-bounds Read		21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/522
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
mdm9205_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/523

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/524					
Improper	21-11-2019	7.2	Out of bound access due to	https://ww	O-QUA-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Restriction of Operations within the Bounds of a Memory Buffer			lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	MDM9-031219/525					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/526					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/527

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	<p>Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2289</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/528
Improper	21-11-2019	2.1	Information disclosure due	https://www	O-QUA-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Restriction of Operations within the Bounds of a Memory Buffer			to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	MDM9-031219/529					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/530					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/531					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/532					
msm8909_firmware										
Loop with Unreachable Exit Condition ('Infinite	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-031219/533					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	lletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/534					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/535					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/536
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/537

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/538					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/539					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/540					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/541					
mdm9635m_firmware										
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit	https://www.qualcomm.com	O-QUA-MDM9-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Exit Condition ('Infinite Loop')			condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	m.com/company/product-security/bulletins/october-2019-bulletin	031219/542					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/octo	O-QUA-MDM9-031219/543					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	ber-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/544					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read		21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MDM9-031219/545
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

qca9980_firmware

Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCA9-031219/546
----------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266		
sdm429_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/548
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/549

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271					bulletin		
Improper Authentication		21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SDM4-031219/550
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/551					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/552					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/553					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/554					
sdm632_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/555					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/556					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/557					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/558					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/559
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/560

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					ct-security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-		O-QUA-SDM6-031219/561
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315						bulletin		
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SDM6-031219/562
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		

msm8917_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/563
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/564
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/565

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/566					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/567					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/568					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130 CVE ID : CVE-2019-2295		
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/569
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer	https://www.qualcomm.com	O-QUA-MSM8-

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315						m.com/company/product-security/bulletins/october-2019-bulletin		031219/570
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-		O-QUA-MSM8-031219/571
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	bulletin	
msm8920_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/572

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/573

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/574
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/576					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/577					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/578					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/579

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/580

msm8937_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/581
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/582					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/583
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	O-QUA-MSM8-031219/584

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	lletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-MSM8-031219/585					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/586					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/587					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/588					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/589					
msm8940_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/590					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/591					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/592

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/593					
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
on			result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/594					
Improper Restriction of Operations within the Bounds of a	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	O-QUA- MSM8- 031219/595					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	lletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/596					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/597					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MSM8-031219/598
msm8996_firmware											
Use After Free		21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-MSM8-031219/599
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	ct-security/bulletins/october-2019-bulletin						
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/600					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/601					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		
sdm450_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/602

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/603					
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/604					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/605					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/606					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/607
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed	https://www.qualcomm.com/	O-QUA-SDM4-031219/608

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					pany//produ ct- security/bu lletins/octo ber-2019- bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,					https://ww w.qualcom m.com/com pany//produ ct- security/bu lletins/octo ber-2019-		O-QUA-SDM4-031219/609
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	bulletin						
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/610					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		

sm8250_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/611
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/612
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/613

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/614					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/615					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/616

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM82-031219/617					
sxr2130_firmware										
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit	https://www.qualcomm	O-QUA-SXR2-031219/618					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Exit Condition ('Infinite Loop')			condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	m.com/company/product-security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/octo	O-QUA-SXR2-031219/619					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	ber-2019-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/620
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/621

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/622					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/623
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/624

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/625					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/626					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/627					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR2-031219/628					
apq8016_firmware										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/629					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		

sa6155p_firmware

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SA61-031219/630
--	------------	-----	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
sc8180x_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SC81-031219/631					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SC81-031219/632					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SC81-031219/633					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SC81-031219/634					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SC81-031219/635					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		
sdm850_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/636

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/637					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/638					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/639					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/640					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/641

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/642					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM8-031219/643					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	security/bulletins/october-2019-bulletin						
mdm915_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/644					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/645					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/646					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289		

qcm2150_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCM2-031219/647
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCM2-031219/648					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCM2-031219/649					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read		21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCM2-031219/650
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		

sdx55_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5-031219/651
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5-031219/652
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5-031219/653

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2339		
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2271</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX5-031219/654
Improper	21-11-2019	10	Lack of integrity check	https://www	O-QUA-SDX5-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authentication			allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/655					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/produ	O-QUA-SDX5-031219/656					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	ct-security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-SDX5-031219/657					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	bulletin	
apq8064_firmware					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-APQ8-031219/658
apq8096_firmware					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,	https://www.qualcomm.com/com	O-QUA-APQ8-031219/659

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Out-of- bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	O-QUA-APQ8- 031219/660					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	bulletin	

sda660_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/661
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/662

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	<p>Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130</p> <p>CVE ID : CVE-2019-10490</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/663
Improper Validation of Array Index	21-11-2019	4.6	<p>Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/664

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/665
Buffer Copy without Checking Size of Input ('Classic Buffer	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	lletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/667					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/668

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/669					
Improper Restriction of	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG	https://www.qualcomm.com/	O-QUA-SDA6-031219/670					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Operations within the Bounds of a Memory Buffer			buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	pany/produ ct-security/bulletins/october-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/671					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/672					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDA6-031219/673

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
sdm439_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/674

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/675					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/676					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/677					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/678					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/679					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/680

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM4-031219/681					
sdm630_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/682					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/683					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/684
Buffer Copy without Checking Size of Input	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/685

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Classic Buffer Overflow')			potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/686					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/687

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/688

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/689					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/690					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/691					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

sdm660_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/692
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/693					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/694
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/695

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	lletins/octo ber-2019- bulletin	
Out-of- bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/696
Buffer Copy without Checking	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility	https://www.qualcomm.com/	O-QUA-SDM6-031219/697

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Size of Input ('Classic Buffer Overflow')			that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	pany/produ ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/698					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/699					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/700

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/701					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/702					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/703					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDM6-031219/704
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		
snapdragon_high_med_2016_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/705

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2335		
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2271</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/706
Improper	21-11-2019	10	Lack of integrity check	https://www	O-QUA-SNAP-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authentication			allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/707					
Improper Restriction of Operations	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/708					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/products-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/709					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/710					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SNAP-031219/711					
mdm9150_firmware										
Use After	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to	https://www.qualcomm.com	O-QUA-MDM9-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Free			static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	m.com/company/product-security/bulletins/october-2019-bulletin	031219/712					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/713					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/714					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

mdm9640_firmware

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/715
--	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/716					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/717
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/718

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/719					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/720					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/721
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MDM9-031219/722

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
msm8909w_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/723

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/724					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/725

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	<p>Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20</p> <p>CVE ID : CVE-2019-10503</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/726
Use After Free	21-11-2019	4.6	<p>Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/727

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/728					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/729

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-MSM8-031219/730
qcs605_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/731					
Improper Restriction of Operations within the	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/732					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	security/bulletins/october-2019-bulletin						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/733					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/734
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/735

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	ber-2019-bulletin						
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/736					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/737					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/738

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/739
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/740

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/741					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/742

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/743
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/744

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/745					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/746
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-QCS6-031219/747					
sdx20_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/748					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/749					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
				QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free		21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SDX2-031219/750	
Improper Validation of		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due				https://www.qualcomm		O-QUA-SDX2-031219/751	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Array Index			to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	m.com/company/product-security/bulletins/october-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/752					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20 CVE ID : CVE-2019-10535		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/753
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/754

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/755
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/756

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/757					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/758					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/759					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
sm7150_firmware					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/760

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/761					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/762					
Time-of-check Time-of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://www.qualcomm.com/com	O-QUA-SM71-031219/763					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
(TOCTOU) Race Condition			modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/764					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/766
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/767

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/768					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/769					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/770
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SM71-031219/771					
sxr1130_firmware										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/772					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Improper Restriction of Operations within the Bounds of a Memory Buffer		21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		O-QUA-SXR1-031219/773
Buffer Copy		21-11-2019	7.2	If a bitmap file is loaded					https://ww		O-QUA-SXR1-
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
without Checking Size of Input ('Classic Buffer Overflow')			from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/774					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/775					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/776					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/777					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/778					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SXR1-031219/779
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization	https://www.qualcomm.com/	O-QUA-SXR1-031219/780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	pany//produ ct- security/bu lletins/octo ber-2019- bulletin						
sdx24_firmware										
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whiltelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	O-QUA-SDX2-031219/781					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	O-QUA-SDX2-031219/782					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	ber-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/783					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/784
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/785

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/786
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA	https://www.qualcomm.com/	O-QUA-SDX2-031219/787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/788					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	lletins/octo ber-2019- bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	O-QUA-SDX2-031219/789					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	O-QUA-SDX2-031219/790					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

Schneider-electric

bmx_p34x_firmware

Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-BMX_-031219/791
----------------------	------------	---	---	---	-----------------------

bmx_noe_0100_firmware

Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium	https://www.schneider-electric.com/ww/en/download/doc	O-SCH-BMX_-031219/792
----------------------	------------	---	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	ument/SEV D-2019-281-02/						
bmx_noe_0110_firmware										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEV D-2019-281-02/	O-SCH-BMX_-031219/793					
bmx_noc_0401_firmware										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules -	https://www.schneider-electric.com/ww/en/download/document/SEV D-2019-281-02/	O-SCH-BMX_-031219/794					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852		

tsx_p57x_firmware

Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-TSX-031219/795
----------------------	------------	---	---	---	----------------------

tsx_ety_x103_firmware

Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-TSX-031219/796
----------------------	------------	---	--	---	----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852		
140_cpu6x_firmware					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-140-031219/797
140_noe_771x1_firmware					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-140-031219/798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unsecure network. CVE ID : CVE-2019-6852		
140_noc_78x00_firmware					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-140_-031219/799
140_noc_77101_firmware					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	O-SCH-140_-031219/800

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ztehome					
c520v21_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-11-2019	5	permission and access control vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can construct a URL for directory traversal and access to other unauthorized files or resources. CVE ID : CVE-2019-3423	http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1011842	O-ZTE-C520-031219/801
Improper Authentication	18-11-2019	6.4	authentication issues vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can automatically obtain access to web services from the authorized browser of the same computer and perform operations. CVE ID : CVE-2019-3424	http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1011842	O-ZTE-C520-031219/802
Hardware					
Lenovo					
thinkpad_usb-c_dock					
N/A	20-11-2019	5	A potential vulnerability reported in ThinkPad USB-C Dock Firmware version 3.7.2 may allow a denial of service. CVE ID : CVE-2019-6176	N/A	H-LEN-THIN-031219/803
thinkagile_7x82					
Improper Neutralization of Special Elements in	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could	N/A	H-LEN-THIN-031219/804

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		

thinkagile_7y11

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/805
--	------------	---	---	-----	-----------------------

thinkagile_7y12

Improper Neutralization of Special Elements in Output Used by a Downstream	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store	N/A	H-LEN-THIN-031219/806
--	------------	---	--	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinkagile_7y88					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/807
thinkagile_7y92					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in	N/A	H-LEN-THIN-031219/808

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinkagile_7z03					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/809
thinksystem_sd530					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is	N/A	H-LEN-THIN-031219/810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinksystem_sd650					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/811
thinksystem_sn550					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.	N/A	H-LEN-THIN-031219/812

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6187		
thinksystem_sn850					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/813
thinksystem_sr150					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/814
thinksystem_sr158					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/815

thinksystem_sr250

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/816
--	------------	---	---	-----	-----------------------

thinksystem_sr258

Improper Neutralization of Special	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity	N/A	H-LEN-THIN-031219/817
------------------------------------	------------	---	--	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		

thinksystem_sr850

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/818
--	------------	---	---	-----	-----------------------

thinksystem_sr860

Improper Neutralization of Special Elements in Output Used by a	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately	N/A	H-LEN-THIN-031219/819
---	------------	---	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Downstream Component ('Injection')			<p>permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.</p> <p>CVE ID : CVE-2019-6187</p>		
thinksystem_st250					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	<p>A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server.</p> <p>CVE ID : CVE-2019-6187</p>	N/A	H-LEN-THIN-031219/820
thinksystem_st258					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	<p>A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational</p>	N/A	H-LEN-THIN-031219/821

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		

thinkagile_7d1h

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/822
--	------------	---	---	-----	-----------------------

thinkagile_7x83

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV	N/A	H-LEN-THIN-031219/823
--	------------	---	---	-----	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinkagile_7y13					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/824
thinkagile_7y14					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the	N/A	H-LEN-THIN-031219/825

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server. CVE ID : CVE-2019-6187		
thinkagile_7y90					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/826
thinkagile_7y93					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/827

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

Weakness	Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
thinkagile_7y94										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187				N/A		H-LEN-THIN-031219/828	
thinkagile_7z04										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187				N/A		H-LEN-THIN-031219/829	
thinkagile_7z05										
Improper Neutralization	20-11-2019	4	A stored CSV Injection vulnerability was reported				N/A		H-LEN-THIN-031219/830	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements in Output Used by a Downstream Component ('Injection')			in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinkagile_7z06					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/831
thinkagile_7z07					
Improper Neutralization of Special Elements in Output Used	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or	N/A	H-LEN-THIN-031219/832

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinkagile_7z20					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/833
thinkagile_yx84					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain	N/A	H-LEN-THIN-031219/834

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinksystem_sr530					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/835
thinksystem_sr550					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being	N/A	H-LEN-THIN-031219/836

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187		
thinksystem_sr570					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/837
thinksystem_sr590					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself	N/A	H-LEN-THIN-031219/838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			and has no effect on the server. CVE ID : CVE-2019-6187							
thinksystem_sr630										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/839					
thinksystem_sr650										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/840					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
thinksystem_st550										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/841					
thinksystem_st558										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/842					
_thinksystem_sr670										
Improper Neutralization	20-11-2019	4	A stored CSV Injection vulnerability was reported	N/A	H-LEN-_THI-031219/843					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
n of Special Elements in Output Used by a Downstream Component ('Injection')			in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187							
thinksystem_sr950										
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-11-2019	4	A stored CSV Injection vulnerability was reported in Lenovo XClarity Controller (XCC) that could allow an administrative or other appropriately permissioned user to store malformed data in certain XCC server informational fields, that could result in crafted formulas being stored in an exported CSV file. The crafted formula is not executed on XCC itself and has no effect on the server. CVE ID : CVE-2019-6187	N/A	H-LEN-THIN-031219/844					
Linksys										
velop_whw0303										
Authorization Bypass Through User-	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct	N/A	H-LIN-VELO-031219/845					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Controlled Key			request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340							
velop_whw0302										
Authorization Bypass Through User-Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340	N/A	H-LIN-VELO-031219/846					
velop_whw0301										
Authorization Bypass Through User-Controlled Key	21-11-2019	6.4	Belkin Linksys Velop 1.1.8.192419 devices allows remote attackers to discover the recovery key via a direct request for the /sysinfo_json.cgi URI. CVE ID : CVE-2019-16340	N/A	H-LIN-VELO-031219/847					
phicomm										
k2\ (psg1218\)										
Improper Input Validation	18-11-2019	9	/usr/lib/lua/luci/controller/admin/autoupgrade.lua on PHICOMM K2(PSG1218) V22.5.9.163 devices allows remote authenticated users to execute any command via shell metacharacters in the cgi-bin/luci autoUpTime parameter. CVE ID : CVE-2019-19117	N/A	H-PHI-K2\(-031219/848					
Qualcomm										
mdm9206										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop	https://www.qualcomm.com/company/produ	H-QUA-MDM9-031219/849					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Infinite Loop')			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	ct-security/bulletins/october-2019-bulletin						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MDM9-031219/850					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486					bulletin		
Use After Free		21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MDM9-031219/851
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/852
Buffer Copy without Checking Size of Input ('Classic	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/853

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	security/bulletins/october-2019-bulletin	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2266		
Out-of-bounds Read	21-11-2019	7.5	<p>Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150</p> <p>CVE ID : CVE-2019-2268</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/855
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/856

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/857					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/858					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/859

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/860					
mdm9607										
Loop with Unreachable Exit	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met	https://www.qualcomm.com/com	H-QUA-MDM9-031219/861					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Condition ('Infinite Loop')			resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	H-QUA- MDM9- 031219/862					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/863					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/864
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/865

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	ct-security/bulletins/october-2019-bulletin	
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/866

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150 CVE ID : CVE-2019-2266		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/867
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/868

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/869					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/870					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of- bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA- MDM9- 031219/871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/872					
msm8909w										
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit	https://www.qualcomm.com	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Exit Condition ('Infinite Loop')			condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	m.com/company/product-security/bulletins/october-2019-bulletin	031219/873					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octo	H-QUA-MSM8-031219/874					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	ber-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/875					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/876					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub	https://www.qualcomm.com/	H-QUA-MSM8-031219/877					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA- MSM8- 031219/878					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/879					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/880					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
msm8996au					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/881

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/882
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-031219/883

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	lletins/october-2019-bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/884					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/885
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/886

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/887					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/888					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/890					
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can	https://www.qualcomm.com/	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
on			result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/891					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA- MSM8- 031219/892					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	lletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/893					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/894					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/895					
qca6574au										
Improper Restriction of Operations within the Bounds of a	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCA6-031219/896					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Memory Buffer			Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	lletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6-031219/897					
Out-of-	21-11-2019	7.5	Possible OOB read issue in	https://ww	H-QUA-QCA6-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/898					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6-031219/899					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
qcs405					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/900

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/901					
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/902					
Buffer Copy without	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported	https://www.qualcomm.com	H-QUA-QCS4-031219/903					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Checking Size of Input ('Classic Buffer Overflow')			rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	m.com/company/product-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/904					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/905
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/906

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/907

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/908
qcs605					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/910					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/911
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/912

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490					ber-2019-bulletin		
Improper Restriction of Operations within the Bounds of a Memory Buffer		21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-QCS6-031219/913
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20 CVE ID : CVE-2019-10535		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/915

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/916					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/917					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/918
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/919

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271					security/bulletins/october-2019-bulletin		
Improper Authentication		21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-		H-QUA-QCS6-031219/920
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/921					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/922					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/923

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/924					
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS6-031219/925					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	lletins/october-2019-bulletin	
sda660					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/926

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/927
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting	https://www.qualcomm.com/	H-QUA-SDA6-031219/928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/929					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/930
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/931

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/932					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink	https://www.qualcomm.com	H-QUA-SDA6-031219/933					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	m.com/company/product-security/bulletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in	https://www.qualcomm.com/company/product-	H-QUA-SDA6-031219/934					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	security/bulletins/october-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-SDA6-031219/935					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/936					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/937					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA6-031219/938					
sdm439										
Loop with Unreachable	21-11-2019	5	While processing Attach Reject message, Valid exit	https://www.qualcomm.com	H-QUA-SDM4-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Exit Condition ('Infinite Loop')			condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	m.com/company/product-security/bulletins/october-2019-bulletin	031219/939					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/octo	H-QUA-SDM4-031219/940					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486						ber-2019-bulletin		
Out-of-bounds Read		21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SDM4-031219/941
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/942					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/943					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295		
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/944

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	<p>While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2315</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/945
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/946

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	ct-security/bulletins/october-2019-bulletin	

sdm630

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/947
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/948					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/949
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/950

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/951					
Out-of-	21-11-2019	10	Buffer over read can happen	https://ww	H-QUA-SDM6-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/952					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication	https://ww w.qualcom m.com/com pany/produ	H-QUA-SDM6-031219/953					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ct- security/bu lletins/octo ber-2019- bulletin						
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/954					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	ber-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/955					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/956					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
sdm660					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/957

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/958					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to	https://www.qualcomm.com	H-QUA-SDM6-031219/959					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	m.com/company/product-security/bulletins/october-2019-bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/960					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/962

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/963					
Out-of-	21-11-2019	10	Buffer over read can happen	https://ww	H-QUA-SDM6-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/964					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/965					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ct- security/bu lletins/octo ber-2019- bulletin						
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo	H-QUA-SDM6- 031219/966					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	ber-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/967					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/968					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/969
sdx20					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/970					
Time-of-check Time-of-use (TOCTOU) Race	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/971					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Condition			bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/972					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SDX2-031219/973
Improper		21-11-2019	2.1	Improper validation for loop					https://ww		H-QUA-SDX2-
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/974
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/975
Buffer Copy without Checking	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates	https://www.qualcomm.com/	H-QUA-SDX2-031219/976

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Size of Input ('Classic Buffer Overflow')			element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	pany/produ ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/977					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/978

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/979

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/980					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/981					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

mdm9150

Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/982
----------------	------------	-----	---	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/983					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/984					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
mdm9640					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/985

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/986					
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/987					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/988
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-031219/989

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	lletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MDM9-031219/990					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289					bulletin		
Integer Underflow (Wrap or Wraparound)		21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MDM9-031219/991
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/992					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		

mdm9650

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/993
--	------------	---	--	---	-----------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/994					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting	https://www.qualcomm.com/	H-QUA-MDM9-031219/995					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/996					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/997
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/999					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1000					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1001

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1002					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1003					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	security/bulletins/october-2019-bulletin						
sdx24										
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1004					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1005

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1006					
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1007					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1008
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1009

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	ber-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1010					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1011					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1012
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX2-031219/1013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303	security/bulletins/october-2019-bulletin	
ipq4019					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-IPQ4-031219/1014

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	bulletin	
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ4-031219/1015

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ipq8064					
Use After Free	21-11-2019	4.6	<p>Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150</p> <p>CVE ID : CVE-2019-2266</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ8-031219/1016
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	<p>Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ8-031219/1017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
ipq8074										
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-IPQ8-031219/1018					
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will	https://www.qualcomm.com/com	H-QUA-IPQ8-031219/1019					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	pany/product-security/bulletins/october-2019-bulletin	
qca6174a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6-031219/1020

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6-031219/1021
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA6-031219/1022

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150</p> <p>CVE ID : CVE-2019-2297</p>		

qca9377

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	<p>Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9-031219/1023
--	------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9-031219/1024
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9-031219/1025

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
qca9379										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9-031219/1026					
Out-of-	21-11-2019	7.5	Possible OOB read issue in P2P action frames while	https://www.qualcomm.com	H-QUA-QCA9-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	m.com/company/product-security/bulletins/october-2019-bulletin	031219/1027					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA9-031219/1028					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		

snapdragon_high_med_2016

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1029
--	------------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1030

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1031

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1032					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1033					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1034					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SNAP-031219/1035

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2318							
apq8009										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1036					
Time-of-check Time-	21-11-2019	4.4	Race condition due to the lack of resource lock which	https://www.qualcomm	H-QUA-APQ8-031219/1037					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
of-use (TOCTOU) Race Condition				will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486						m.com/company/product-security/bulletins/october-2019-bulletin		
Use After Free		21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-APQ8-031219/1038
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1039

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20 CVE ID : CVE-2019-10503		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1040
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1041

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1042					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1043					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1044
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1045

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-APQ8-031219/1046
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		
apq8098					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1047

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1048					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1049

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	<p>Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20</p> <p>CVE ID : CVE-2019-10503</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1050
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	<p>Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1051

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1052
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1053

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1054					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1055					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1056					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1057					
msm8939										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1058					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1059					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1060					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1061					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1062					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		

msm8953

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1063
--	------------	---	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1064
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1065

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490					security/bulletins/october-2019-bulletin		
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1066
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1067					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1068					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1069
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1070

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1071
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1072					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		
msm8998					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1073

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	<p>Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150</p> <p>CVE ID : CVE-2019-10486</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1074
Use After Free	21-11-2019	2.1	<p>Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1075

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1076					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1077
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1078

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1079
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1080

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1081					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1082					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1083
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1084

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1085
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		
nicobar					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1086

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1087					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1088

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1089
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1090

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1091
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1092

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	ber-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1093					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1094					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-NICO-031219/1095					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

apq8053

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1096
--	------------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1097					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to	https://www.qualcomm.com	H-QUA-APQ8-031219/1098					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490					m.com/company/product-security/bulletins/october-2019-bulletin		
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-APQ8-031219/1099
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1100
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-APQ8-031219/1101

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1102
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1103

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1104					
Out-of-	21-11-2019	10	Buffer over read can happen	https://ww	H-QUA-APQ8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
bounds Read			while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/1105					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication	https://ww w.qualcom m.com/com pany/produ	H-QUA-APQ8- 031219/1106					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ct- security/bu lletins/octo ber-2019- bulletin						
Improper Restriction of Operations within the Bounds of a Memory	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1107					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	ber-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1108					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1109					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1110					
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary	https://www.qualcomm.com	H-QUA-APQ8-031219/1111					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	m.com/company/product-security/bulletins/october-2019-bulletin	

mdm9207c

Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1112
---	------------	-----	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1113

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1114
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1115

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1116
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1117

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	ber-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1118					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150 CVE ID : CVE-2019-2297		
msm8905					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1119

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1120					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1121					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1122					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1123
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1124

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1125					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1126					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1127					
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary	https://www.qualcomm.com	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					m.com/company/product-security/bulletins/october-2019-bulletin		031219/1128
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute,					https://www.qualcomm.com/company/product-security/bulletins/octo		H-QUA-MSM8-031219/1129
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	ber-2019- bulletin	

qcn7605

Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1130
---	------------	-----	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1131					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1132					
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1133					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1134
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCN7-031219/1135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		

sdm845

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1136
--	------------	---	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1137
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1138

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1139					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1140
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1141

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1142					
Use After	21-11-2019	4.6	Possible double free issue in	https://ww	H-QUA-SDM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
Free				kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266				w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin		031219/1143	
Out-of- bounds Read		21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710,				https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin		H-QUA-SDM8- 031219/1144	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1145

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1146					
Improper Restriction of	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG	https://www.qualcomm.com/	H-QUA-SDM8-031219/1147					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Operations within the Bounds of a Memory Buffer			buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	pany/produ ct-security/bulletins/october-2019-bulletin						
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1148					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read		21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1149
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1150

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1151					
apq8017										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1152					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1153					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1154
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	lletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1156					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1157
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1158

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1159					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1160					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1161
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1162

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					ct-security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-		H-QUA-APQ8-031219/1163
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	bulletin						
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1164					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318		

apq8096au

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1165
--	------------	---	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1166
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1167

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490						security/bulletins/october-2019-bulletin		
Improper Validation of Array Index		21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-APQ8-031219/1168
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1169
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1171
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	bulletin	
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1173

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2271</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1174
Improper	21-11-2019	10	Lack of integrity check	https://www	H-QUA-APQ8-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authentication			allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/1175					
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1176					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
)				Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297						ct-security/bulletins/october-2019-bulletin		
Out-of-bounds Read		21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-APQ8-031219/1177
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1178					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1179					
msm8976										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1180					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Infinite Loop')			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MSM8-031219/1181					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1182					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1183					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		
sda845					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1184

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1185
Time-of-check Time-of-use	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1186

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
(TOCTOU) Race Condition			modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1187					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Improper validation for loop variable received from firmware can lead to out of bound access in WLAN function while iterating through loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, APQ8098, MDM9640, MSM8996AU, MSM8998, QCA6574AU, QCN7605, QCS405, QCS605, SDA845, SDM845, SDX20 CVE ID : CVE-2019-10535	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1188
Buffer Copy without Checking Size of Input	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1189

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Classic Buffer Overflow')			than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	ct-security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1190					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1191					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1192

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1193
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1195					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1196					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDA8-031219/1197					
sdm636										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1198					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1199					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1200
Out-of-bounds Read	21-11-2019	4.6	Buffer over-read can occur in fast message handler due to improper input validation while processing a message from firmware in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1201

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, SDA660, SDM636, SDM660, SDX20, SDX24 CVE ID : CVE-2019-10563	ber-2019-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1202
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1203

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SDM6- 031219/1204					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1205					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1206					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130 CVE ID : CVE-2019-2295		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1207
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1208

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1209					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		

sdm670

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1210
--	------------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1211
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1212

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	security/bulletins/october-2019-bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1213					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1214
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1216					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1217					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1218

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2295		
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1219
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer,	https://www.qualcomm.com/com	H-QUA-SDM6-031219/1220

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	pany/produ ct- security/bu lletins/octo ber-2019- bulletin						
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-SDM6-031219/1221					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	bulletin	
sdm710					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1222

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1223
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1224

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1225					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1226
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1227

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of- bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150 CVE ID : CVE-2019-2268	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1228
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1229

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	ct- security/bu lletins/octo ber-2019- bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1230					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	ber-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1231					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1232					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1233					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM7-031219/1234					
qca8081										
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCA8-031219/1235					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318							
qcs404										
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/1236					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/1237					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016, SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/1238
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCS4-031219/1239

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	lletins/october-2019-bulletin						
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCS4-031219/1240					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329		
sxr1130					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2335		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1242
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1243

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1244					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1246
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1247

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1248
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR1-031219/1249					
sm6150										
Loop with Unreachable Exit	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met	https://www.qualcomm.com/com	H-QUA-SM61-031219/1250					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Condition ('Infinite Loop')			resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	pany//product-security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-SM61-031219/1251					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1252
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1253

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1254					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1256

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	bulletin	
Out-of-bounds Read	21-11-2019	7.5	Possible OOB read issue in P2P action frames while handling WLAN management frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1257

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2268		
Out-of-bounds Read	21-11-2019	10	<p>Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2271</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1258
Improper	21-11-2019	10	Lack of integrity check	https://www	H-QUA-SM61-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Authentication			allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	w.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	031219/1259					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1260					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date		CVSS	Description & CVE ID						Patch		NCIIPC ID	
					Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303						ct-security/bulletins/october-2019-bulletin			
N/A		21-11-2019		7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-		H-QUA-SM61-031219/1261	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	bulletin	
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM61-031219/1262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329		
sm8150					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1263

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1264
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1265
Time-of-check Time-of-use (TOCTOU)	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1266

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Race Condition			statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	ct-security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1267					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1269					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1270					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1271					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1272

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2289		
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	<p>Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150</p> <p>CVE ID : CVE-2019-2297</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1273
Out-of-bounds Read	21-11-2019	7.5	<p>SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1274

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1275					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM81-031219/1276					
mdm9615										
Loop with Unreachable Exit Condition ('Infinite	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1277					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Loop')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1278					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1279					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1280					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
mdm9625					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1281

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1282					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1283					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1284					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
mdm9205					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1285

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1286
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1287

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1288					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1289					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1290					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1291					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1292					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1293					
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to	https://www.qualcomm.com	H-QUA-MDM9-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	m.com/company/product-security/bulletins/october-2019-bulletin	031219/1294

msm8909

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1295
--	------------	---	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	<p>Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20</p> <p>CVE ID : CVE-2019-10503</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1297
Use After Free	21-11-2019	4.6	<p>Possible double free issue in kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064,</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1299					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1300

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			, SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1301					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1302					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1303
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
mdm9655					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1304

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1305					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1306					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1307					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
mdm9635m					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1308

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1310

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-11-2019	7.5	<p>SNDP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2303</p>	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1311
qca9980					
Use After Free	21-11-2019	4.6	Possible double free issue in kernel while handling the camera sensor and its sub	https://www.qualcomm.com/com	H-QUA-QCA9-031219/1312

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	

qm215

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1313
--	------------	---	---	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1314					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1315

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1316

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1317					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1318					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1319					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QM21-031219/1320

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2318							
sm7150										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1321					
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further	https://www.qualcomm.com	H-QUA-SM71-031219/1322					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	m.com/company/product-security/bulletins/october-2019-bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1323					
Time-of-check Time-of-use (TOCTOU) Race Condition	21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM71-031219/1324					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	lletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1325					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1326					
Use After	21-11-2019	4.6	Possible double free issue in	https://www	H-QUA-SM71-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Free			kernel while handling the camera sensor and its sub modules power sequence in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MSM8909, MSM8909W, Nicobar, QCA9980, QCS405, QCS605, SDM845, SDX24, SM7150, SM8150 CVE ID : CVE-2019-2266	w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/1327					
Out-of- bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019- bulletin	H-QUA-SM71- 031219/1328					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1329					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1330					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SM71-031219/1331
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM71-031219/1332					
sdm429										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1333					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
				MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Time-of-check Time-of-use (TOCTOU) Race Condition		21-11-2019	4.4	Race condition due to the lack of resource lock which will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630,				https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SDM4-031219/1334	
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1335					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1336

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1337					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1338					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1339					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1340

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2318							
sdm632										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1341					
Time-of-check Time-	21-11-2019	4.4	Race condition due to the lack of resource lock which	https://www.qualcomm	H-QUA-SDM6-031219/1342					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
of-use (TOCTOU) Race Condition			will be concurrently modified in the memcpy statement leads to out of bound access in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150 CVE ID : CVE-2019-10486	m.com/company/product-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1343					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1344					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1345					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1346					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1347

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM6-031219/1348
msm8917					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1349

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1350					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1351
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-031219/1352

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	lletins/october-2019-bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MSM8-031219/1353					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	bulletin						
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1354					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1355					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1356					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1357					
msm8920										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1358					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1359					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1360

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1361					
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
on			result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/1362					
Improper Restriction of Operations within the Bounds of a	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA- MSM8- 031219/1363					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	lletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	7.5	SNDCCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1364					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1365					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1366					
msm8937										
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1367					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Infinite Loop')			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	ct-security/bulletins/october-2019-bulletin						
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MSM8-031219/1368					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	bulletin						
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1369					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1370					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130, SXR2130 CVE ID : CVE-2019-2271		
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1371

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1372					
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1373					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1374					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2315		
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1375

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-2318							
msm8940										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1376					
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to	https://www.qualcomm.com	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	m.com/company/product-security/bulletins/october-2019-bulletin	031219/1377					
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1378					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503							
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1379					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1380					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289		
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1381
Out-of-bounds Read	21-11-2019	7.5	SNDSCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1382

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303					security/bulletins/october-2019-bulletin		
N/A		21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1383
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID						Patch		NCIIPC ID
				Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315								
Out-of-bounds Read		21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-MSM8-031219/1384
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318							
msm8996										
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MSM8-031219/1385					
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer	https://www.qualcomm.com	H-QUA-MSM8-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	m.com/company/product-security/bulletins/october-2019-bulletin	031219/1386					
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-MSM8-031219/1387					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	bulletin	
sdm450					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1389

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 CVE ID : CVE-2019-10490		
Improper Validation of Array Index	21-11-2019	4.6	Out-of-bounds access can occur in camera driver due to improper validation of array index in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, SDA660, SDM450, SDM630, SDM636, SDM660, SDX20 CVE ID : CVE-2019-10503	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1390
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1391

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

Weakness		Publish Date	CVSS	Description & CVE ID						Patch	NCIIPC ID
				APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication		21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205,						https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1392
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1393					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1394					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1395

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM4-031219/1396
sm8250					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1397

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1398					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1399
Buffer Copy without Checking Size of Input ('Classic Buffer	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM82-031219/1400

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	lletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1401					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1402					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SM82-031219/1403					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303		
sxr2130					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1404

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1405
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1406

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 CVE ID : CVE-2019-2339		
Use After Free	21-11-2019	2.1	Use after free issue in Xtra daemon shutdown due to static object instance getting freed from a multiple places in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS605, SDA660, SDA845, SDM450, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10490	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1407
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	4.6	Buffer overflow can occur in wlan module if supported rates or extended rates element length is greater than max rate set length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-SXR2-031219/1408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM670, SDM710, SDM845, SDX20, SM6150, SM8150, SM8250, SXR2130 CVE ID : CVE-2019-10566	bulletin						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1409					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1410

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1411					
Out-of-bounds Read	21-11-2019	7.5	SNDTCP module may access array out side its boundary when it receives malformed	https://www.qualcomm.com/	H-QUA-SXR2-031219/1412					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303	pany//produ ct- security/bu lletins/octo ber-2019- bulletin						
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://ww w.qualcom m.com/com pany/produ ct- security/bu lletins/octo ber-2019-	H-QUA-SXR2-031219/1413					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315	bulletin						
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SXR2-031219/1414					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329							
apq8016										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1415					
sa6155p										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SA61-031219/1416					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251		
sc8180x					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SC81-031219/1417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SC81-031219/1418

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SC81-031219/1419					
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SC81-031219/1420					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
on			result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289	pany//produ ct- security/bu lletins/octo ber-2019- bulletin						
Out-of- bounds Read	21-11-2019	7.5	SNDACP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://ww w.qualcom m.com/com pany/produ ct- security/bu	H-QUA-SC81- 031219/1421					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303	lletins/october-2019-bulletin	
sdm850					
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1422

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

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335							
Improper Restriction of Operations within the Bounds of a Memory Buffer		21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845,					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SDM8-031219/1423
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-11-2019	7.2	If a bitmap file is loaded from any un-authenticated source, there is a possibility that the bitmap can potentially cause stack buffer overflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8016, APQ8096AU, APQ8098, MDM9205, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, SA6155P, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 CVE ID : CVE-2019-2251	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1424					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1425					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness		Publish Date	CVSS	Description & CVE ID					Patch		NCIIPC ID
				Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication		21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon					https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin		H-QUA-SDM8-031219/1426
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-11-2019	2.1	Information disclosure due to lack of address range check done on the SysDBG buffers in SDI code. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1427					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			MDM9205, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, Snapdragon_High_Med_2016 , SXR1130 CVE ID : CVE-2019-2295							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1428					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDM8-031219/1429					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315							
mdm915										
Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1430					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-MDM9-031219/1431					
Improper Authenticati	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can	https://www.qualcomm.com/	H-QUA-MDM9-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			<p>result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130</p> <p>CVE ID : CVE-2019-2289</p>	pany/produ ct- security/bu lletins/octo ber-2019- bulletin	031219/1432
qcm2150					
Loop with Unreachable Exit Condition	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop	https://ww w.qualcom m.com/com pany/produ	H-QUA- QCM2- 031219/1433

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
('Infinite Loop')			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2335	ct-security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-	H-QUA-QCM2-031219/1434					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271	bulletin						
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCM2-031219/1435					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-QCM2-031219/1436					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2303		

sdx55

Loop with Unreachable Exit Condition ('Infinite Loop')	21-11-2019	5	While processing Attach Reject message, Valid exit condition is not met resulting into an infinite loop in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1437
--	------------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016, SXR1130, SXR2130 CVE ID : CVE-2019-2335		
Use After Free	21-11-2019	4.9	Subsequent use of the CBO listener may result in further memory corruption due to use after free issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, SDX55, SM6150, SM7150, SM8150, SXR2130 CVE ID : CVE-2019-2336	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1438
Improper Restriction of Operations within the	21-11-2019	7.2	Out of bound access due to lack of check of whitelist array size while reading the image elf segments. in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1439

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2339	security/bulletins/october-2019-bulletin						
Out-of-bounds Read	21-11-2019	10	Buffer over read can happen while parsing downlink session management OTA messages if network sends un-intended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1440					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2271							
Improper Authentication	21-11-2019	10	Lack of integrity check allows MODEM to accept any NAS messages which can result into authentication bypass of NAS in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1441					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2289							
Out-of-bounds Read	21-11-2019	7.5	SNDCP module may access array out side its boundary when it receives malformed XID message. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8976, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1442					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2303							
Use After Free	21-11-2019	7.2	Use after free issue in cleanup routine due to missing pointer sanitization for a failed start of a trusted application. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9205, QCS404, QCS605, SDA845, SDM670, SDM710, SDM845, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130 CVE ID : CVE-2019-2329	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-SDX5-031219/1443					
apq8064										
Integer Underflow (Wrap or Wraparound)	21-11-2019	4.6	Buffer overflow can occur while processing non-standard NAN message from user space. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1444					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150 CVE ID : CVE-2019-2297		

apq8096

N/A	21-11-2019	7.2	While invoking the API to copy from fd or local buffer to the secure buffer, Parameters being populated are from non secure environment. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1445
-----	------------	-----	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 , SXR1130, SXR2130 CVE ID : CVE-2019-2315		
Out-of-bounds Read	21-11-2019	2.1	Non Secure Kernel can cause Trustzone to do an arbitrary memory read which will result into DOS in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8096, APQ8096AU, IPQ8074, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, QCA8081, QM215, SDM429, SDM439, SDM450, SDM632, Snapdragon_High_Med_2016 CVE ID : CVE-2019-2318	https://www.qualcomm.com/company/product-security/bulletins/october-2019-bulletin	H-QUA-APQ8-031219/1446

Schneider-electric

bm_x_p34x

Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	H-SCH-BMX_-031219/1447
----------------------	------------	---	--	---	------------------------

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852		
bmx_noe_0100					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	H-SCH-BMX_-031219/1448
bmx_noe_0110					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	H-SCH-BMX_-031219/1449

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			of the controller on an unsecure network. CVE ID : CVE-2019-6852							
bmx_noc_0401										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	H-SCH-BMX_-031219/1450					
tsx_p57x										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/	H-SCH-TSX_-031219/1451					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Patch		NCIIPC ID	
tsx_ety_x103										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852				https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/		H-SCH-TSX_-031219/1452	
140_cpu6x										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852				https://www.schneider-electric.com/ww/en/download/document/SEVD-2019-281-02/		H-SCH-140_-031219/1453	
140_noe_771x1										
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists				https://www.schneider		H-SCH-140_-031219/1454	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	- electric.com /ww/en/download/document/SEV D-2019-281-02/	
140_noc_78x00					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules, Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	https://www.schneider- electric.com /ww/en/download/document/SEV D-2019-281-02/	H-SCH-140_- 031219/1455
140_noc_77101					
Information Exposure	20-11-2019	5	A CWE-200: Information Exposure vulnerability exists in Modicon Controllers (M340 CPUs, M340 communication modules,	https://www.schneider- electric.com /ww/en/do	H-SCH-140_- 031219/1456

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Premium CPUs, Premium communication modules, Quantum CPUs, Quantum communication modules - see security notification for specific versions), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network. CVE ID : CVE-2019-6852	wnload/document/SEVD-2019-281-02/	
ztehome					
c520v21					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-11-2019	5	permission and access control vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can construct a URL for directory traversal and access to other unauthorized files or resources. CVE ID : CVE-2019-3423	http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1011842	H-ZTE-C520-031219/1457
Improper Authentication	18-11-2019	6.4	authentication issues vulnerability, which exists in V2.1.14 and below versions of C520V21 smart camera devices. An attacker can automatically obtain access to web services from the authorized browser of the same computer and perform operations. CVE ID : CVE-2019-3424	http://support.zte.com.cn/support/news/Loo pholeInfoDetail.aspx?newsId=1011842	H-ZTE-C520-031219/1458

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