Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Adobe					
dreamweaver					
Untrusted Search Path	18-07-2019	6.8	Adobe Dreamweaver direct download installer versions 19.0 and below, 18.0 and below have an Insecure Library Loading (DLL hijacking) vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user. **CVE ID : CVE-2019-7956**	N/A	A-ADO-DREA-130819/1
bridge_cc					
Out-of-bounds Read	18-07-2019	4.3	Adobe Bridge CC version 9.0.2 and earlier versions have an out of bound read vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-7963**	N/A	A-ADO-BRID-130819/2
campaign					
Improper Input Validation	18-07-2019	5	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Insufficient input validation vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-7843**	N/A	A-ADO-CAMP-130819/3
N/A	18-07-2019	5	Adobe Campaign Classic	N/A	A-ADO-CAMP-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 18.10.5-8984 and earlier versions have an Improper error handling vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-7846**		130819/4
Improper Restriction of XML External Entity Reference ('XXE')	18-07-2019	5	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Improper Restriction of XML External Entity Reference ('XXE') vulnerability. Successful exploitation could lead to Arbitrary read access to the file system in the context of the current user. **CVE ID : CVE-2019-7847**	N/A	A-ADO-CAMP-130819/5
Improper Access Control	18-07-2019	5	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Inadequate access control vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-7848**	N/A	A-ADO-CAMP-130819/6
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-07-2019	7.5	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have a Command injection vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user. **CVE ID : CVE-2019-7850**	N/A	A-ADO-CAMP-130819/7
Informatio	18-07-2019	5	Adobe Campaign Classic	N/A	A-ADO-CAMP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			version 18.10.5-8984 and earlier versions have an Information Exposure Through an Error Message vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user. **CVE ID : CVE-2019-7941**		130819/8
experience_manager					
Cross-Site Request Forgery (CSRF)	18-07-2019	4.3	Adobe Experience Manager version 6.4 and ealier have a Cross-Site Request Forgery vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user. **CVE ID : CVE-2019-7953**	N/A	A-ADO-EXPE-130819/9
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-07-2019	4.3	Adobe Experience Manager version 6.4 and ealier have a Stored Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user. **CVE ID : CVE-2019-7954**	N/A	A-ADO-EXPE-130819/10
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-07-2019	5.8	Adobe Experience Manager version 6.4 and ealier have a Reflected Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user. **CVE ID : CVE-2019-7955**	N/A	A-ADO-EXPE-130819/11
ajdg					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
adrotate					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	6.5	The AJdG AdRotate plugin before 5.3 for WordPress allows SQL Injection. **CVE ID : CVE-2019-13570**	https://ajdg.solutions/2019/07/11/adrotate-pro-5-3-important-update-for-security-and-ads-txt/	A-AJD-ADRO-130819/12
akeo					
rufus					
Uncontrolled Search Path Element	19-07-2019	6.8	Akeo Consulting Rufus 3.0 and earlier is affected by: DLL search order hijacking. The impact is: Arbitrary code execution WITH escalation of privilege. The component is: Executable installers, portable executables (ALL executables on the web site). The attack vector is: CAPEC-471, CWE-426, CWE-427. **CVE ID : CVE-2019-1010100**	N/A	A-AKE-RUFU-130819/13
N/A	19-07-2019	7.5	Akeo Consulting Rufus 3.0 and earlier is affected by: Insecure Permissions. The impact is: arbitrary code execution with escalation of privilege. The component is: Executable installer, portable executable (ALL executables available). The attack vector is: CWE-29, CWE-377, CWE-379. **CVE ID : CVE-2019-1010101**	N/A	A-AKE-RUFU-130819/14
Altn					
mdaemon_email_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-07-2019	5	MDaemon Email Server 19 skips SpamAssassin checks by default for e-mail messages larger than 2 MB (and limits checks to 10 MB even with special configuration), which is arguably inconsistent with currently popular message sizes. This might interfere with risk management for malicious e-mail, if a customer deploys a server with sufficient resources to scan large messages. **CVE ID : CVE-2019-13612**	N/A	A-ALT-MDAE-130819/15
antsword_project					
antsword					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	In antSword before 2.1.0, self-XSS in the database configuration leads to code execution via modules/database/asp/index.js, modules/database/custom/index.js, modules/database/index.js, or modules/database/php/index.js. **CVE ID : CVE-2019-13970**	N/A	A-ANT-ANTS-130819/16
Avast					
antivirus					
Improper Link Resolution Before File Access ('Link Following')	18-07-2019	3.6	In Avast Antivirus before 19.4, a local administrator can trick the product into renaming arbitrary files by replacing the Logs\Update.log file with a symlink. The next time the product attempts to write to the log file, the target of the	N/A	A-AVA-ANTI-130819/17

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			symlink is renamed. This defect can be exploited to rename a critical product file (e.g., AvastSvc.exe), causing the product to fail to start on the next system restart. **CVE ID : CVE-2019-11230**		
axiosys					
bento4					
NULL Pointer Dereference	18-07-2019	4.3	In Bento4 1.5.1-627, AP4_DataBuffer::SetDataSize does not handle reallocation failures, leading to a memory copy into a NULL pointer. This is different from CVE-2018-20186. **CVE ID : CVE-2019-13959**	N/A	A-AXI-BENT-130819/18
b3log					
wide					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-07-2019	5	b3log Wide before 1.6.0 allows three types of attacks to access arbitrary files. First, the attacker can write code in the editor, and compile and run it approximately three times to read an arbitrary file. Second, the attacker can create a symlink, and then place the symlink into a ZIP archive. An unzip operation leads to read access, and write access (depending on file permissions), to the symlink target. Third, the attacker can import a Git repository that contains a symlink, similarly leading to read and write access.	N/A	A-B3L-WIDE-130819/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13915		
bacnet_protocol_stack_project					
bacnet_protocol_stack					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	6.8	BACnet Stack bacserv 0.9.1 and 0.8.5 is affected by: Buffer Overflow. The impact is: exploit was not explored. The component is: bacserv BVLC forwarded NPDU. bvlc_bdt_forward_npdu() calls bvlc_encode_forwarded_npdu( ) which copies the content from the request into a local in the bvlc_bdt_forward_npdu() stack frame and clobbers the canary. The attack vector is: A BACnet/IP device with BBMD enabled based on this library connected to IP network. The fixed version is: 0.8.6. **CVE ID : CVE-2019-1010073**	N/A	A-BAC-BACN-130819/20
cat_runner_decorate_home_project					
cat_runner_decorate_home					
Improper Input Validation	22-07-2019	5	The application API of Cat Runner Decorate Home version 2.8.0 for Android does not sufficiently verify inputs that are assumed to be immutable but are actually externally controllable. Attackers can manipulate users' score parameters exchanged between client and server. **CVE ID : CVE-2019-13097**	N/A	A-CAT-CAT_-130819/21
centos-webpanel					
centos_web_panel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	16-07-2019	8.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, a cwpsrv-xxx cookie allows a normal user to craft and upload a session file to the /tmp directory, and use it to become the root user. **CVE ID : CVE-2019-13359**	N/A	A-CEN-CENT-130819/22
Improper Authentication	16-07-2019	7.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, remote attackers can bypass authentication in the login process by leveraging knowledge of a valid username. **CVE ID : CVE-2019-13360**	N/A	A-CEN-CENT-130819/23
Information Exposure	16-07-2019	5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, the Login process allows attackers to check whether a username is valid by reading the HTTP response. **CVE ID : CVE-2019-13383**	N/A	A-CEN-CENT-130819/24
Improper Authentication	16-07-2019	6.5	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.838 to 0.9.8.846, remote attackers can bypass authentication in the login process by leveraging the knowledge of a valid username. The attacker must defeat an encoding that is not equivalent to base64, and thus this is different from CVE-2019-13360. **CVE ID : CVE-2019-13605**	N/A	A-CEN-CENT-130819/25
central_dogma_project					
central_dogma					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-07-2019	4.3	Cross-site scripting vulnerability in Central Dogma 0.17.0 to 0.40.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2019-6002**	N/A	A-CEN-CENT-130819/26
Cherokee-project					
cherokee_webserver					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	5	Cherokee Webserver Latest Cherokee Web server Upto Version 1.2.103 (Current stable) is affected by: Buffer Overflow - CWE-120. The impact is: Crash. The component is: Main cherokee command. The attack vector is: Overwrite argv[0] to an insane length with execl. The fixed version is: There's no fix yet. **CVE ID : CVE-2019-1010218**	N/A	A-CHE-CHER-130819/27
Cisco					
vision_dynamic_signage_director					
Improper Authentication	17-07-2019	10	A vulnerability in the REST API interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to bypass authentication on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could	N/A	A-CIS-VISI-130819/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to execute arbitrary actions through the REST API with administrative privileges on the affected system. The REST API is enabled by default and cannot be disabled. **CVE ID : CVE-2019-1917**		
findit_network_manager					
Use of Hard-coded Credentials	17-07-2019	7.2	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root-level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable. **CVE ID : CVE-2019-1919**	N/A	A-CIS-FIND-130819/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
industrial_network_director					
N/A	17-07-2019	4.3	A vulnerability in the Web Services Management Agent (WSMA) feature of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data using an invalid X.509 certificate. The vulnerability is due to insufficient X.509 certificate validation when establishing a WSMA connection. An attacker could exploit this vulnerability by supplying a crafted X.509 certificate during the WSMA connection setup phase. A successful exploit could allow the attacker to conduct man-in-the-middle attacks to decrypt confidential information on WSMA connections to the affected software. At the time of publication, this vulnerability affected Cisco IND Software releases prior to 1.7. **CVE ID : CVE-2019-1940**	N/A	A-CIS-INDU-130819/30
identity_services_engine					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface	N/A	A-CIS-IDEN-130819/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. At the time of publication, this vulnerability affected Cisco ISE running software releases prior to 2.4.0 Patch 9 and 2.6.0. **CVE ID : CVE-2019-1941**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	4	A vulnerability in the sponsor portal web interface for Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. At the time of publication, this vulnerability affected Cisco ISE running software releases	N/A	A-CIS-IDEN-130819/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.6.0 and prior. **CVE ID : CVE-2019-1942**		
findit_network_probe					
Use of Hard-coded Credentials	17-07-2019	7.2	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root-level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable. **CVE ID : CVE-2019-1919**	N/A	A-CIS-FIND-130819/33
cjson_project					
cjson					
Improper Check for Unusual or Exceptiona	19-07-2019	5	DaveGamble/cJSON cJSON 1.7.8 is affected by: Improper Check for Unusual or Exceptional Conditions. The	N/A	A-CJS-CJSO-130819/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
l Conditions			impact is: Null dereference, so attack can cause denial of service. The component is: cJSON_GetObjectItemCaseSensitive() function. The attack vector is: crafted json file. The fixed version is: 1.7.9 and later. **CVE ID : CVE-2019-1010239**		
Cmsmadesimple					
Bable:multilingual_site					
URL Redirection to Untrusted Site ('Open Redirect')	16-07-2019	5.8	Babel: Multilingual site Babel All is affected by: Open Redirection. The impact is: Redirection to any URL, which is supplied to redirect.php in a "newurl" parameter. The component is: redirect.php. The attack vector is: The victim must open a link created by an attacker. Attacker may use any legitimate site using Babel to redirect user to a URL of his/her choosing. **CVE ID : CVE-2019-1010290**	N/A	A-CMS-BABL-130819/35
code42					
code42					
Improper Access Control	19-07-2019	6.5	In Code42 for Enterprise through 6.8.4, an administrator without web restore permission but with the ability to manage users in an organization can impersonate a user with web restore permission. When requesting the token to do a web restore, an administrator with permission to manage a user could request the token of	https://support.code42.com/Terms_and_conditions/Code42_customer_support_resources/Code42_security_advisories/Privilege_Es	A-COD-CODE-130819/36

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that user. If the administrator was not authorized to perform web restores but the user was authorized to perform web restores, this would allow the administrator to impersonate the user with greater permissions. In order to exploit this vulnerability, the user would have to be an administrator with access to manage an organization with a user with greater permissions than themselves. **CVE ID : CVE-2019-11553**	calation_in_LoginToken_API	
Comodo					
antivirus					
N/A	17-07-2019	7.2	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Local Privilege Escalation due to CmdAgent's handling of COM clients. A local process can bypass the signature check enforced by CmdAgent via process hollowing which can then allow the process to invoke sensitive COM methods in CmdAgent such as writing to the registry with SYSTEM privileges. **CVE ID : CVE-2019-3969**	N/A	A-COM-ANTI-130819/37
Improper Input Validation	17-07-2019	2.1	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Arbitrary File Write due to Cavwp.exe handling of Comodo's Antivirus database. Cavwp.exe loads Comodo antivirus definition database in unsecured global section	N/A	A-COM-ANTI-130819/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			objects, allowing a local low privileged process to modify this data directly and change virus signatures. **CVE ID : CVE-2019-3970**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	2.1	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to a local Denial of Service affecting CmdVirth.exe via its LPC port "cmdvrtLPCServerPort". A low privileged local process can connect to this port and send an LPC_DATAGRAM, which triggers an Access Violation due to hardcoded NULLs used for Source parameter in a memcpy operation that is called for this handler. This results in CmdVirth.exe and its child svchost.exe instances to terminate. **CVE ID : CVE-2019-3971**	N/A	A-COM-ANTI-130819/39
Out-of-bounds Read	17-07-2019	2.1	Comodo Antivirus versions 12.0.0.6810 and below are vulnerable to Denial of Service affecting CmdAgent.exe via an unprotected section object "<GUID>_CisSharedMemBuff". This section object is exposed by CmdAgent and contains a SharedMemoryDictionary object, which allows a low privileged process to modify the object data causing CmdAgent.exe to crash. **CVE ID : CVE-2019-3972**	N/A	A-COM-ANTI-130819/40
Out-of-bounds	17-07-2019	4.9	Comodo Antivirus versions 11.0.0.6582 and below are	N/A	A-COM-ANTI-130819/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			vulnerable to Denial of Service affecting CmdGuard.sys via its filter port "cmdServicePort". A low privileged process can crash CmdVirth.exe to decrease the port's connection count followed by process hollowing a CmdVirth.exe instance with malicious code to obtain a handle to "cmdServicePort". Once this occurs, a specially crafted message can be sent to "cmdServicePort" using "FilterSendMessage" API. This can trigger an out-of-bounds write if lpOutBuffer parameter in FilterSendMessage API is near the end of specified buffer bounds. The crash occurs when the driver performs a memset operation which uses a size beyond the size of buffer specified, causing kernel crash. **CVE ID : CVE-2019-3973**		
computerlab					
maple_computer_wbt_snmp_administrator					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	SnmpAdm.exe in MAPLE WBT SNMP Administrator v2.0.195.15 has an Unauthenticated Remote Buffer Overflow via a long string to the CE Remote feature listening on Port 987. **CVE ID : CVE-2019-13577**	N/A	A-COM-MAPL-130819/42
Cpanel					
cpanel					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	3.5	cPanel before 82.0.2 has stored XSS in the WHM Tomcat Manager interface (SEC-504). **CVE ID : CVE-2019-14386**	N/A	A-CPA-CPAN-130819/43
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	4.3	cPanel before 82.0.2 has Self XSS in the cPanel and webmail master templates (SEC-506). **CVE ID : CVE-2019-14387**	N/A	A-CPA-CPAN-130819/44
Improper Input Validation	30-07-2019	5	cPanel before 82.0.2 allows unauthenticated file creation because Exim log parsing is mishandled (SEC-507). **CVE ID : CVE-2019-14388**	N/A	A-CPA-CPAN-130819/45
N/A	30-07-2019	2.1	cPanel before 82.0.2 allows local users to discover the MySQL root password (SEC-510). **CVE ID : CVE-2019-14389**	N/A	A-CPA-CPAN-130819/46
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-07-2019	3.5	cPanel before 82.0.2 has stored XSS in the WHM Modify Account interface (SEC-512). **CVE ID : CVE-2019-14390**	N/A	A-CPA-CPAN-130819/47
N/A	30-07-2019	2.1	cPanel before 82.0.2 does not properly enforce Reseller	N/A	A-CPA-CPAN-130819/48

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
			package creation ACLs (SEC-514). **CVE ID : CVE-2019-14391**		
Improper Input Validation	30-07-2019	6.5	cPanel before 80.0.22 allows remote code execution by a demo account because of incorrect URI dispatching (SEC-501). **CVE ID : CVE-2019-14392**	https://documentation.cpanel.net/display/CL/80+Change+Log	A-CPA-CPAN-130819/49
Dancer::plugin::simplecrud_project					
Dancer::plugin::simplecrud					
Improper Access Control	17-07-2019	4	Dancer::Plugin::SimpleCRUD 1.14 and earlier is affected by: Incorrect Access Control. The impact is: Potential for unathorised access to data. The component is: Incorrect calls to _ensure_auth() wrapper result in authentication-checking not being applied to al routes. **CVE ID : CVE-2019-1010084**	N/A	A-DAN-DANC-130819/50
Dell					
emc_unity_operating_environment					
Improper Authorization	18-07-2019	4	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain an improper authorization vulnerability in NAS Server quotas configuration. A remote authenticated Unisphere Operator could potentially exploit this vulnerability to edit quota configuration of other users. **CVE ID : CVE-2019-3734**	N/A	A-DEL-EMC_-130819/51
Protection	18-07-2019	2.1	Dell EMC Unity and UnityVSA	N/A	A-DEL-EMC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Mechanism Failure			versions prior to 5.0.0.0.5.116 contain a plain-text password storage vulnerability. A Unisphere user?s (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle (logs files for troubleshooting). A local authenticated attacker with access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2019-3741**		130819/52
emc_unityvsa_operating_environment					
Improper Authorization	18-07-2019	4	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain an improper authorization vulnerability in NAS Server quotas configuration. A remote authenticated Unisphere Operator could potentially exploit this vulnerability to edit quota configuration of other users. **CVE ID : CVE-2019-3734**	N/A	A-DEL-EMC_-130819/53
Protection Mechanism Failure	18-07-2019	2.1	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain a plain-text password storage vulnerability. A Unisphere user?s (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle (logs files for troubleshooting). A local authenticated attacker with	N/A	A-DEL-EMC_-130819/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user. **CVE ID : CVE-2019-3741**		
deltaww					
cnssoft_screeneditor					
Out-of-bounds Read	24-07-2019	4.3	Delta Electronics CNCSoft ScreenEditor, Versions 1.00.89 and prior. Multiple out-of-bounds read vulnerabilities may cause information disclosure due to lacking user input validation for processing project files. **CVE ID : CVE-2019-10992**	N/A	A-DEL-CNSS-130819/55
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-07-2019	6.8	Delta Electronics CNCSoft ScreenEditor, Versions 1.00.89 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by processing specially crafted project files, allowing an attacker to remotely execute arbitrary code. There is a lack of user input validation before copying data from project files onto the heap. **CVE ID : CVE-2019-10982**	N/A	A-DEL-CNSS-130819/56
dependencytrack					
dependency-track					
Improper Neutralization of Input During Web Page	29-07-2019	3.5	Dependency-Track before 3.5.1 allows XSS. **CVE ID : CVE-2019-1020007**	https://github.com/DependencyTrack/dependency-track/secu	A-DEP-DEPE-130819/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')				rity/advisories/GHSA-jp9v-w6vw-9m5v	
Dolibarr					
dolibarr					
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	Dolibarr 7.0.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: allow malitious html to change user password, disable users and disable password encryptation. The component is: Function User password change, user disable and password encryptation. The attack vector is: admin access malitious urls. **CVE ID : CVE-2019-1010054**	N/A	A-DOL-DOLI-130819/58
Domainmod					
Domainmod					
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change admin password. The component is: http://127.0.0.1/settings/password/ http://127.0.0.1/admin/users/add.php http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page. **CVE ID : CVE-2019-1010094**	N/A	A-DOM-DOMA-130819/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can add the administrator account. The component is: http://127.0.0.1/admin/users/add.php. The attack vector is: After the administrator logged in, open the html page. **CVE ID : CVE-2019-1010095**	N/A	A-DOM-DOMA-130819/60
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change the read-only user to admin. The component is: http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page. **CVE ID : CVE-2019-1010096**	N/A	A-DOM-DOMA-130819/61
dpic_project					
dpic					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-07-2019	6.8	dpic 2019.06.20 has a Stack-based Buffer Overflow in the wfloat() function in main.c. **CVE ID : CVE-2019-13989**	N/A	A-DPI-DPIC-130819/62
eclass					
eclass_ip					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-07-2019	7.5	eClass platform < ip.2.5.10.2.1 allows an attacker to execute SQL command via /admin/academic/studenview_left.php StudentID parameter. **CVE ID : CVE-2019-9885**	https://zeroday.hitcon.org/vulnerability/ZD-2019-00333	A-ECL-ECLA-130819/63
Eclipse					
openj9					
N/A	17-07-2019	4.6	AIX builds of Eclipse OpenJ9 before 0.15.0 contain unused RPATHs which may facilitate code injection and privilege elevation by local users. **CVE ID : CVE-2019-11771**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=548055	A-ECL-OPEN-130819/64
Out-of-bounds Write	17-07-2019	7.5	In Eclipse OpenJ9 prior to 0.15, the String.getBytes(int, int, byte[], int) method does not verify that the provided byte array is non-null nor that the provided index is in bounds when compiled by the JIT. This allows arbitrary writes to any 32-bit address or beyond the end of a byte array within Java code run under a SecurityManager. **CVE ID : CVE-2019-11772**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=549075	A-ECL-OPEN-130819/65
elcom					
elcom_cms					
Improper Neutralization of Special Elements	19-07-2019	5	Elcom CMS before 10.7 has SQL Injection via EventSearchByState.aspx and EventSearchAdv.aspx. **CVE ID : CVE-2019-12946**	N/A	A-ELC-ELCO-130819/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')					
Espocrm					
espocrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	Stored XSS in EspoCRM before 5.6.4 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The attack begins by storing a new stream message containing an XSS payload. The stored payload can then be triggered by clicking a malicious link on the Notifications page. **CVE ID : CVE-2019-13643**	N/A	A-ESP-ESPO-130819/67
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	An issue was discovered in EspoCRM before 5.6.6. There is stored XSS due to lack of filtration of user-supplied data in Create Task. A malicious attacker can modify the parameter name to contain JavaScript code. **CVE ID : CVE-2019-14329**	N/A	A-ESP-ESPO-130819/68
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create Case. A malicious attacker can modify the firstName and lastName to contain JavaScript code. **CVE ID : CVE-2019-14330**	N/A	A-ESP-ESPO-130819/69
Improper	28-07-2019	4.3	An issue was discovered in	N/A	A-ESP-ESPO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create User. A malicious attacker can modify the firstName and lastName to contain JavaScript code. **CVE ID : CVE-2019-14331**		130819/70
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	EspoCRM version 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the api/v1/Document functionality for storing documents in the account tab. An attacker can upload a crafted file that contains JavaScript code in its name. This code will be executed when a user opens a page of any profile with this. **CVE ID : CVE-2019-14349**	N/A	A-ESP-ESPO-130819/71
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-07-2019	4.3	EspoCRM 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the Knowledge base. A malicious attacker can inject JavaScript code in the body parameter during api/v1/KnowledgeBaseArticle knowledge-base record creation. **CVE ID : CVE-2019-14350**	N/A	A-ESP-ESPO-130819/72
N/A	28-07-2019	4	EspoCRM 5.6.4 is vulnerable to user password hash enumeration. A malicious authenticated attacker can brute-force a user password hash by 1 symbol at a time	N/A	A-ESP-ESPO-130819/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using specially crafted api/v1/User?filterList filters. **CVE ID : CVE-2019-14351**		
Exim					
exim					
N/A	25-07-2019	10	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the ${sort } expansion for items that can be controlled by an attacker (e.g., $local_part or $domain). **CVE ID : CVE-2019-13917**	N/A	A-EXI-EXIM-130819/74
Exiv2					
exiv2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-07-2019	4.3	Exiv2::PngImage::readMetadata() in pngimage.cpp in Exiv2 0.27.99.0 allows attackers to cause a denial of service (heap-based buffer over-read) via a crafted image file. **CVE ID : CVE-2019-14369**	N/A	A-EXI-EXIV-130819/75
Out-of-bounds Read	28-07-2019	4.3	In Exiv2 0.27.99.0, there is an out-of-bounds read in Exiv2::MrwImage::readMetadata() in mrwimage.cpp. It could result in denial of service. **CVE ID : CVE-2019-14370**	N/A	A-EXI-EXIV-130819/76
fanucamerica					
robotics_virtual_robot_controller					
Improper Limitation of a Pathname to a	17-07-2019	5	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 allows Directory Traversal via a forged HTTP request.	N/A	A-FAN-ROBO-130819/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			**CVE ID : CVE-2019-13584**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 has a Buffer Overflow via a forged HTTP request. **CVE ID : CVE-2019-13585**	N/A	A-FAN-ROBO-130819/78
firefly-iii					
firefly_iii					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	Firefly III before 4.7.17.1 is vulnerable to stored XSS due to lack of filtration of user-supplied data in a budget name. The JavaScript code is contained in a transaction, and is executed on the tags/show/tag_number tag summary page. **CVE ID : CVE-2019-13644**	N/A	A-FIR-FIRE-130819/79
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file names. The JavaScript code is executed during attachments/edit/$file_id$ attachment editing. **CVE ID : CVE-2019-13645**	N/A	A-FIR-FIRE-130819/80
Improper Neutralization of Input During Web Page	17-07-2019	3.5	Firefly III before 4.7.17.3 is vulnerable to reflected XSS due to lack of filtration of user-supplied data in a search query.	N/A	A-FIR-FIRE-130819/81

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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')			**CVE ID : CVE-2019-13646**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file content. The JavaScript code is executed during attachments/view/$file_id$ attachment viewing. **CVE ID : CVE-2019-13647**	N/A	A-FIR-FIRE-130819/82
Flatcore					
flatcore					
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	A CSRF vulnerability was found in flatCore before 1.5, leading to the upload of arbitrary .php files via acp/core/files.upload-script.php. **CVE ID : CVE-2019-13961**	N/A	A-FLA-FLAT-130819/83
Foliovision					
fv_flowplayer_video_player					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	10	A SQL injection vulnerability exists in the FolioVision FV Flowplayer Video Player plugin before 7.3.19.727 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system. **CVE ID : CVE-2019-13573**	https://wordpress.org/plugins/fv-wordpress-flowplayer/#developers	A-FOL-FV_F-130819/84
Foxitsoftware					
phantompdf					
Uncontroll	21-07-2019	5	An issue was discovered in	N/A	A-FOX-PHAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ed Resource Consumption			Foxit PhantomPDF before 8.3.11. The application could crash when calling the clone function due to an endless loop resulting from confusing relationships between a child and parent object (caused by an append error). **CVE ID : CVE-2019-14207**		130819/85
NULL Pointer Dereference	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to a NULL pointer dereference and crash when getting a PDF object from a document, or parsing a certain portfolio that contains a null dictionary. **CVE ID : CVE-2019-14208**	N/A	A-FOX-PHAN-130819/86
Improper Restriction of Operations within the Bounds of a Memory Buffer	21-07-2019	7.5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to Heap Corruption due to data desynchrony when adding AcroForm. **CVE ID : CVE-2019-14209**	N/A	A-FOX-PHAN-130819/87
NULL Pointer Dereference	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to Memory Corruption due to the use of an invalid pointer copy, resulting from a destructed string object. **CVE ID : CVE-2019-14210**	N/A	A-FOX-PHAN-130819/88
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could	N/A	A-FOX-PHAN-130819/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash due to the lack of proper validation of the existence of an object prior to performing operations on that object when executing JavaScript. **CVE ID : CVE-2019-14211**		
NULL Pointer Dereference	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash when calling certain XFA JavaScript due to the use of, or access to, a NULL pointer without proper validation on the object. **CVE ID : CVE-2019-14212**	N/A	A-FOX-PHAN-130819/90
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash due to the repeated release of the signature dictionary during CSG_SignatureF and CPDF_Document destruction. **CVE ID : CVE-2019-14213**	N/A	A-FOX-PHAN-130819/91
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.10. The application could be exposed to a JavaScript Denial of Service when deleting pages in a document that contains only one page by calling a "t.hidden = true" function. **CVE ID : CVE-2019-14214**	N/A	A-FOX-PHAN-130819/92
Improper Input Validation	21-07-2019	5	An issue was discovered in Foxit PhantomPDF before 8.3.11. The application could crash when calling xfa.event.rest XFA JavaScript	N/A	A-FOX-PHAN-130819/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to accessing a wild pointer. **CVE ID : CVE-2019-14215**		
Freedesktop					
poppler					
Integer Overflow or Wraparound	22-07-2019	4.3	The JPXStream::init function in Poppler 0.78.0 and earlier doesn't check for negative values of stream length, leading to an Integer Overflow, thereby making it possible to allocate a large memory chunk on the heap, with a size controlled by an attacker, as demonstrated by pdftocairo. **CVE ID : CVE-2019-9959**	https://gitlab.freedesktop.org/poppler/poppler/blob/master/NEWS	A-FRE-POPP-130819/94
frog_cms_project					
frog_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	3.5	Frog CMS 1.1 is affected by: Cross Site Scripting (XSS). The impact is: Cookie stealing, Alert pop-up on page, Redirecting to another phishing site, Executing browser exploits. The component is: Snippets. **CVE ID : CVE-2019-1010235**	N/A	A-FRO-FROG-130819/95
gdnsd					
gdnsd					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	7.5	The set_ipv4() function in zscan_rfc1035.rl in gdnsd 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv4 address in zone data. **CVE ID : CVE-2019-13951**	N/A	A-GDN-GDNS-130819/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-07-2019	7.5	The set_ipv6() function in zscan_rfc1035.rl in gdnsd before 2.4.3 and 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv6 address in zone data. **CVE ID : CVE-2019-13952**	N/A	A-GDN-GDNS-130819/97
Genetechsolutions					
pie_register					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	Genetechsolutions Pie Register 3.0.15 is affected by: Cross Site Scripting (XSS). The impact is: Stealing of session cookies. The component is: File: Login. Parameters: interim-login, wp-lang, and supplied URL. The attack vector is: If a victim clicks a malicious link, the attacker can steal his/her account. The fixed version is: 3.0.16. **CVE ID : CVE-2019-1010207**	N/A	A-GEN-PIE_-130819/98
gitea					
gitea					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-07-2019	4.3	Gitea 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to fix: https://github.com/go-gitea/gitea/pull/5905. The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.	N/A	A-GIT-GITE-130819/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1010261		
glyphandcog					
xpdfreader					
Integer Overflow or Wraparound	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an Integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "one byte per line" case. **CVE ID : CVE-2019-14288**	N/A	A-GLY-XPDF-130819/100
Integer Overflow or Wraparound	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "multiple bytes per line" case. **CVE ID : CVE-2019-14289**	N/A	A-GLY-XPDF-130819/101
Out-of-bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 2. **CVE ID : CVE-2019-14290**	N/A	A-GLY-XPDF-130819/102
Out-of-bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 3. **CVE ID : CVE-2019-14291**	N/A	A-GLY-XPDF-130819/103
Out-of-bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6	N/A	A-GLY-XPDF-130819/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			case 1. **CVE ID : CVE-2019-14292**		
Out-of-bounds Read	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 2. **CVE ID : CVE-2019-14293**	N/A	A-GLY-XPDF-130819/105
Use After Free	27-07-2019	4.3	An issue was discovered in Xpdf 4.01.01. There is a use-after-free in the function JPXStream::fillReadBuf at JPXStream.cc, due to an out of bounds read. **CVE ID : CVE-2019-14294**	N/A	A-GLY-XPDF-130819/106
GNU					
patch					
Improper Link Resolution Before File Access ('Link Following')	17-07-2019	5.8	In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c. **CVE ID : CVE-2019-13636**	N/A	A-GNU-PATC-130819/107
binutils					
Improper Input Validation	23-07-2019	4.3	GNU binutils gold gold v1.11-v1.16 (GNU binutils v2.21-v2.31.1) is affected by: Improper Input Validation, Signed/Unsigned Comparison, Out-of-bounds Read. The impact is: Denial of service. The component is: gold/fileread.cc:497, elfcpp/elfcpp_file.h:644. The attack vector is: An ELF file with an invalid e_shoff header	N/A	A-GNU-BINU-130819/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			field must be opened. **CVE ID : CVE-2019-1010204**		
Integer Overflow or Wraparound	24-07-2019	4.3	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. simple_object_elf_match in simple-object-elf.c does not check for a zero shstrndx value, leading to an integer overflow and resultant heap-based buffer overflow. **CVE ID : CVE-2019-14250**	N/A	A-GNU-BINU-130819/109
gorul					
gourl					
Unrestricted Upload of File with Dangerous Type	23-07-2019	5	GoUrl.io GoURL Wordpress Plugin 1.4.13 and earlier is affected by: CWE-434. The impact is: unauthenticated/unzuthorized Attacker can upload executable file in website. The component is: gourl.php#L5637. The fixed version is: 1.4.14. **CVE ID : CVE-2019-1010209**	N/A	A-GOR-GOUR-130819/110
gpac					
gpac					
Out-of-bounds Read	16-07-2019	5	In GPAC before 0.8.0, isomedia/isom_read.c in libgpac.a has a heap-based buffer over-read, as demonstrated by a crash in gf_m2ts_sync in media_tools/mpegts.c. **CVE ID : CVE-2019-13618**	N/A	A-GPA-GPAC-130819/111
Haproxy					
haproxy					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-07-2019	5	HAProxy through 2.0.2 allows attackers to cause a denial of service (ha_panic) via vectors related to htx_manage_client_side_cookies in proto_htx.c. **CVE ID : CVE-2019-14241**	N/A	A-HAP-HAPR-130819/112
helm					
helm					
Improper Certificate Validation	17-07-2019	7.5	helm Before 2.7.2 is affected by: CWE-295: Improper Certificate Validation. The impact is: Unauthorized clients could connect to the server because self-signed client certs were aloowed. The component is: helm (many files updated, see https://github.com/helm/helm/pull/3152/files/1096813bf9a425e2aa4ac755b6c991b626dfab50). The attack vector is: A malicious client could connect to the server over the network. The fixed version is: 2.7.2. **CVE ID : CVE-2019-1010275**	N/A	A-HEL-HELM-130819/113
hisiphp					
hisiphp					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-07-2019	4.3	hisiphp 1.0.8 is affected by: Cross Site Scripting (XSS). **CVE ID : CVE-2019-1010193**	N/A	A-HIS-HISI-130819/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
HP					
arcsight_logger					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-07-2019	4.3	Mitigates a stored cross site scripting issue in ArcSight Logger versions prior to 6.7.1 **CVE ID : CVE-2019-3485**	N/A	A-HP-ARCS-130819/115
icewall_sso_agent					
Improper Input Validation	19-07-2019	7.1	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7. **CVE ID : CVE-2019-11989**	N/A	A-HP-ICEW-130819/116
mfa_proxy					
Improper Input Validation	19-07-2019	7.1	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and	N/A	A-HP-MFA_-130819/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7. **CVE ID : CVE-2019-11989**		
universal_internet_of_things					
Improper Access Control	19-07-2019	9	Security vulnerabilities in HPE UIoT versions 1.6, 1.5, 1.4.2, 1.4.1, 1.4.0, and 1.2.4.2 could allow unauthorized remote access and access to sensitive data. HPE has addressed this issue in HPE UIoT: * For customers with release UIoT 1.6, fixes are made available with 1.6 RP603 * For customers with release UIoT 1.5, fixes are made available with 1.5 RP503 HF3 * For customers with release older than 1.5, such as 1.4.0, 1.4.1, 1.4.2 and 1.2.4.2, the resolution will be to upgrade to 1.5 RP503 HF3 or 1.6 RP603 Customers are requested to upgrade to the updated versions or contact HPE support for further assistance. **CVE ID : CVE-2019-11990**	N/A	A-HP-UNIV-130819/118
ht2labs					
learning_locker					
Improper Neutralization of Input During	16-07-2019	4.3	In HT2 Labs Learning Locker 3.15.1, it's possible to inject malicious HTML and JavaScript code into the DOM of the website via the	N/A	A-HT2-LEAR-130819/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			PATH_INFO to the dashboards/ URI. **CVE ID : CVE-2019-12834**		
IBM					
spectrum_protect					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.2	The IBM Spectrum Protect 7.1 and 8.1 Backup-Archive Client is vulnerable to a buffer overflow. This could allow execution of arbitrary code on the local system or the application to crash. IBM X-Force ID: 160200. **CVE ID : CVE-2019-4267**	N/A	A-IBM-SPEC-130819/120
maximo_asset_management					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-07-2019	5	IBM Maximo Asset Management 7.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 162887. **CVE ID : CVE-2019-4430**	https://www.ibm.com/support/docview.wss?uid=ibm10959173	A-IBM-MAXI-130819/121
qradar_security_information_and_event_manager					
Information Exposure	17-07-2019	2.1	IBM QRadar SIEM 7.2 and 7.3 could allow a local user to obtain sensitive information when exporting content that could aid an attacker in further attacks against the system. IBM X-Force ID: 156563. **CVE ID : CVE-2019-4054**	https://www.ibm.com/support/docview.wss?uid=ibm10957139	A-IBM-QRAD-130819/122
Improper Neutralizat	17-07-2019	3.5	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site	https://www.ibm.com	A-IBM-QRAD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion of Input During Web Page Generation ('Cross-site Scripting')			scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159131. **CVE ID : CVE-2019-4211**	/support/docview.wss?uid=ibm10957143	130819/123
Cross-Site Request Forgery (CSRF)	25-07-2019	6.8	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 159132. **CVE ID : CVE-2019-4212**	https://www.ibm.com/support/docview.wss?uid=ibm10959463	A-IBM-QRAD-130819/124
cloud_private					
Information Exposure	25-07-2019	2.1	IBM Cloud Private 2.1.0, 3.1.0, and 3.1.1 could disclose highly sensitive information in installer logs that could be use for further attacks against the system. IBM X-Force ID: 158115. **CVE ID : CVE-2019-4116**	N/A	A-IBM-CLOU-130819/125
N/A	25-07-2019	4.6	IBM Cloud Private 3.1.1 and 3.1.2 could allow a local user to obtain elevated privileges due to improper security context constraints. IBM X-Force ID: 162706. **CVE ID : CVE-2019-4415**	N/A	A-IBM-CLOU-130819/126
Session Fixation	25-07-2019	4.6	IBM Cloud Private 3.1.0, 3.1.1, and 3.1.2 does not invalidate session after logout which	https://www.ibm.com/support/d	A-IBM-CLOU-130819/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow a local user to impersonate another user on the system. IBM X-Force ID: 162949. **CVE ID : CVE-2019-4439**	ocview.wss?uid=ibm10884892	
jazz_for_service_management					
Improper Access Control	17-07-2019	4	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 is missing function level access control that could allow a user to delete authorized resources. IBM X-Force ID: 159033. **CVE ID : CVE-2019-4194**	N/A	A-IBM-JAZZ-130819/128
icegram					
email_subscribers_&_newsletters					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	10	A SQL injection vulnerability exists in the Icegram Email Subscribers & Newsletters plugin through 4.1.7 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system. **CVE ID : CVE-2019-13569**	N/A	A-ICE-EMAI-130819/129
I-doit					
i-doit					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	18-07-2019	7.5	Synetics GmbH I-doit 1.12 and earlier is affected by: SQL Injection. The impact is: Unauthenticated mysql database access. The component is: Web login form. The attack vector is: An attacker can exploit the vulnerability by sending a	N/A	A-I-D-I-DO-130819/130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			malicious HTTP POST request. The fixed version is: 1.12.1. **CVE ID : CVE-2019-1010248**		
Ilias					
ilias					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	4.3	Ilias 5.3 before 5.3.12; 5.2 before 5.2.21 is affected by: Cross Site Scripting (XSS) - CWE-79 Type 2: Stored XSS (or Persistent). The impact is: Execute code in the victim's browser. The component is: Assessment / TestQuestionPool. The attack vector is: Cloze Test Text gap (attacker) / Corrections view (victim). The fixed version is: 5.3.12. **CVE ID : CVE-2019-1010237**	N/A	A-ILI-ILIA-130819/131
jeesite					
jeesite					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	4	Jeesite 1.2.7 is affected by: SQL Injection. The impact is: sensitive information disclosure. The component is: updateProcInsIdByBusinessId() function in src/main/java/com.thinkgem.jeesite/modules/act/ActDao.java has SQL Injection vulnerability. The attack vector is: network connectivity,authenticated. The fixed version is: 4.0 and later. **CVE ID : CVE-2019-1010201**	N/A	A-JEE-JEES-130819/132
Jenkins					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
credentials_binding					
N/A	19-07-2019	4	Jenkins Credentials Binding Plugin Jenkins 1.17 is affected by: CWE-257: Storing Passwords in a Recoverable Format. The impact is: Authenticated users can recover credentials. The component is: config-variables.jelly line #30 (passwordVariable). The attack vector is: Attacker creates and executes a Jenkins job. **CVE ID : CVE-2019-1010241**	N/A	A-JEN-CRED-130819/133
jenkins					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-07-2019	4	A path traversal vulnerability in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java allowed attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build. **CVE ID : CVE-2019-10352**	N/A	A-JEN-JENK-130819/134
Cross-Site Request Forgery (CSRF)	17-07-2019	5.1	CSRF tokens in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier did not expire, thereby allowing attackers able to obtain them to bypass CSRF protection. **CVE ID : CVE-2019-10353**	N/A	A-JEN-JENK-130819/135
Informatio	17-07-2019	4	A vulnerability in the Stapler web framework used in	N/A	A-JEN-JENK-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			Jenkins 2.185 and earlier, LTS 2.176.1 and earlier allowed attackers to access view fragments directly, bypassing permission checks and possibly obtain sensitive information. **CVE ID : CVE-2019-10354**		130819/136
jsish					
jsish					
NULL Pointer Dereference	23-07-2019	4.3	jsish 2.4.74 2.0474 is affected by: CWE-476: NULL Pointer Dereference. The impact is: denial of service. The component is: function Jsi_StrcmpDict (jsiChar.c:121). The attack vector is: The victim must execute crafted javascript code. The fixed version is: 2.4.77. **CVE ID : CVE-2019-1010162**	https://jsish.org/fossil/jsi/tktview/5533c4d665b9683eebe4d662493f15eb911d1c8f	A-JSI-JSIS-130819/137
Out-of-bounds Read	23-07-2019	5	Jsish 2.4.77 2.0477 is affected by: Out-of-bounds Read. The impact is: denial of service. The component is: function lexer_getchar (jsiLexer.c:9). The attack vector is: executing crafted javascript code. The fixed version is: 2.4.78. **CVE ID : CVE-2019-1010169**	N/A	A-JSI-JSIS-130819/138
Use After Free	23-07-2019	5	Jsish 2.4.77 2.0477 is affected by: Use After Free. The impact is: denial of service. The component is: function Jsi_ObjFree (jsiObj.c:230). The attack vector is: executing crafted javascript code. The fixed version is: 2.4.78.	https://jsish.org/fossil/jsi/tktview/870f496bb8a707491df8026e2ff78b33a5cf44c1	A-JSI-JSIS-130819/139

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
			CVE ID : CVE-2019-1010170		
NULL Pointer Dereference	23-07-2019	5	Jsish 2.4.83 2.0483 is affected by: Nullpointer dereference. The impact is: denial of service. The component is: function jsi_DumpFunctions (jsiEval.c:567). The attack vector is: executing crafted javascript code. The fixed version is: 2.4.84. **CVE ID : CVE-2019-1010171**	https://jsish.org/fossil/jsi/tktview/a3026a7c06e0f41af461aa0bc2f7a7e886209390	A-JSI-JSIS-130819/140
Improper Input Validation	23-07-2019	5	Jsish 2.4.84 2.0484 is affected by: Reachable Assertion. The impact is: denial of service. The component is: function Jsi_ValueArrayIndex (jsiValue.c:366). The attack vector is: executing crafted javascript code. The fixed version is: after commit 738ead193aff380a7e3d7ffb8e11e446f76867f3. **CVE ID : CVE-2019-1010173**	https://jsish.org/fossil/jsi/tktview/b3278d1a441477d50363d28df79bbf58de2448af	A-JSI-JSIS-130819/141
Kaspersky					
anti-virus					
Information Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 **CVE ID : CVE-2019-8286**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#110719	A-KAS-ANTI-130819/142

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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_anti-virus					
Information Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 **CVE ID : CVE-2019-8286**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#110719	A-KAS-FREE-130819/143
internet_security					
Information Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 **CVE ID : CVE-2019-8286**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#110719	A-KAS-INTE-130819/144
small_office_security					
Information Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link).	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#110719	A-KAS-SMAL-130819/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability has CVSS v3.0 base score 2.6 **CVE ID : CVE-2019-8286**		
total_security					
Information Exposure	18-07-2019	4.3	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6 **CVE ID : CVE-2019-8286**	https://support.kaspersky.com/general/vulnerability.aspx?el=12430#110719	A-KAS-TOTA-130819/146
knot-resolver					
knot_resolver					
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver component of knot resolver through version 3.2.0 before 4.1.0 which allows remote attackers to bypass DNSSEC validation for non-existence answer. NXDOMAIN answer would get passed through to the client even if its DNSSEC validation failed, instead of sending a SERVFAIL packet. Caching is not affected by this particular bug but see CVE-2019-10191. **CVE ID : CVE-2019-10190**	https://www.knot-resolver.cz/2019-07-10-knot-resolver-4.1.0.html	A-KNO-KNOT-130819/147
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver of knot resolver before version 4.1.0 which allows remote attackers	https://www.knot-resolver.cz/2019-07-	A-KNO-KNOT-130819/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to downgrade DNSSEC-secure domains to DNSSEC-insecure state, opening possibility of domain hijack using attacks against insecure DNS protocol. **CVE ID : CVE-2019-10191**	10-knot-resolver-4.1.0.html	
ladon_project					
ladon					
Improper Restriction of XML External Entity Reference ('XXE')	18-07-2019	7.5	Ladon since 0.6.1 (since ebef0aae48af78c159b6fce81bc6f5e7e0ddb059) is affected by: XML External Entity (XXE). The impact is: Information Disclosure, reading files and reaching internal network endpoints. The component is: SOAP request handlers. For instance: https://bitbucket.org/jakobsg/ladon/src/42944fc012a3a48214791c120ee5619434505067/src/ladon/interfaces/soap.py#lines-688. The attack vector is: Send a specially crafted SOAP call. **CVE ID : CVE-2019-1010268**	N/A	A-LAD-LADO-130819/149
layerbb					
layerbb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	LayerBB 1.1.3 allows XSS via the application/commands/new.php pm_title variable, a related issue to CVE-2019-17997. **CVE ID : CVE-2019-13972**	N/A	A-LAY-LAYE-130819/150
Unrestricte	19-07-2019	7.5	LayerBB 1.1.3 allows	N/A	A-LAY-LAYE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Upload of File with Dangerous Type			admin/general.php arbitrary file upload because the custom_logo filename suffix is not restricted, and .php may be used. **CVE ID : CVE-2019-13973**		130819/151
Cross-Site Request Forgery (CSRF)	19-07-2019	6.8	LayerBB 1.1.3 allows conversations.php/cmd/new CSRF. **CVE ID : CVE-2019-13974**	N/A	A-LAY-LAYE-130819/152
Libav					
libav					
N/A	28-07-2019	4.3	An issue was discovered in Libav 12.3. There is an infinite loop in the function mov_probe in the file libavformat/mov.c, related to offset and tag. **CVE ID : CVE-2019-14371**	N/A	A-LIB-LIBA-130819/153
N/A	28-07-2019	4.3	In Libav 12.3, there is an infinite loop in the function wv_read_block_header() in the file wvdec.c. **CVE ID : CVE-2019-14372**	N/A	A-LIB-LIBA-130819/154
Libreoffice					
libreoffice					
Improper Input Validation	17-07-2019	7.5	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into executing arbitrary python	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9848	A-LIB-LIBR-130819/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9848**		
Information Exposure	17-07-2019	4	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9849**	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9849	A-LIB-LIBR-130819/156
libsdl					
libsdl					
Out-of-bounds	16-07-2019	6.8	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x	N/A	A-LIB-LIBS-130819/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			through 2.0.9 has a heap-based buffer over-read in BlitNtoN in video/SDL_blit_N.c when called from SDL_SoftBlit in video/SDL_blit.c. **CVE ID : CVE-2019-13616**		
Libssh2					
libssh2					
Integer Overflow or Wraparound	16-07-2019	5.8	In libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855. **CVE ID : CVE-2019-13115**	N/A	A-LIB-LIBS-130819/158
linagora					
hublin					
Improper Limitation of a Pathname to a Restricted Directory ('Path	23-07-2019	5	LINAGORA hublin latest (commit 72ead897082403126bf8df9264e70f0a9de247ff) is affected by: Directory Traversal. The impact is: The vulnerability allows an attacker to access any file (with a fixed extension) on the server. The	N/A	A-LIN-HUBL-130819/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			component is: A web-view renderer; details here: https://lgtm.com/projects/g/linagora/hublin/snapshot/af9f1ce253b4ee923ff8da8f9d908d02a8e95b7f/files/backend/webserver/views.js?sort=name&dir=ASC&mode=heatmap&showExcluded=false#xb24eb0101d2aec21:1. The attack vector is: Attacker sends a specially crafted HTTP request. **CVE ID : CVE-2019-1010205**		
Llnl					
model_specific_registers-safe					
Improper Access Control	18-07-2019	5	Lawrence Livermore National Laboratory msr-safe v1.1.0 is affected by: Incorrect Access Control. The impact is: An attacker could modify model specific registers. The component is: ioctl handling. The attack vector is: An attacker could exploit a bug in ioctl interface whitelist checking, in order to write to model specific registers, normally a function reserved for the root user. The fixed version is: v1.2.0. **CVE ID : CVE-2019-1010066**	N/A	A-LLN-MODE-130819/160
lodash					
lodash					
Uncontrolled Resource Consumption	17-07-2019	4	lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler.	N/A	A-LOD-LODA-130819/161

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
			The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11. **CVE ID : CVE-2019-1010266**		
logmeininc					
join.me					
Improper Input Validation	17-07-2019	9.3	In LogMeIn join.me before 3.16.0.5505, an attacker could execute arbitrary commands on a targeted system. This vulnerability is due to unsafe search paths used by the application URI that is defined in Windows. An attacker could exploit this vulnerability by convincing a targeted user to follow a malicious link. Successful exploitation could cause the application to load libraries from the directory targeted by the URI link. The attacker could use this behavior to execute arbitrary commands on the system with the privileges of the targeted user if the attacker can place a crafted library in a directory that is accessible to the vulnerable system. **CVE ID : CVE-2019-13637**	N/A	A-LOG-JOIN-130819/162
mailcleaner					
mailcleaner					
Information Exposure	18-07-2019	5	MailCleaner before c888fbb6aaa7c5f8400f637bcf1cbb844de46cd9 is affected by: Unauthenticated MySQL	N/A	A-MAI-MAIL-130819/163

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			database password information disclosure. The impact is: MySQL database content disclosure (e.g. username, password). The component is: The API call in the function allowAction() in NewslettersController.php. The attack vector is: HTTP Get request. The fixed version is: c888fbb6aaa7c5f8400f637bcf1cbb844de46cd9. **CVE ID : CVE-2019-1010246**		
marginalia_project					
marginalia					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24-07-2019	7.5	marginalia < 1.6 is affected by: SQL Injection. The impact is: The impact is a injection of any SQL queries when a user controller argument is added as a component. The component is: Affects users that add a component that is user controller, for instance a parameter or a header. The attack vector is: Hacker inputs a SQL to a vulnerable vector(header, http parameter, etc). The fixed version is: 1.6. **CVE ID : CVE-2019-1010191**	N/A	A-MAR-MARG-130819/164
Mcafee					
agent					
N/A	18-07-2019	4.6	Privilege escalation vulnerability in McAfee Agent (MA) before 5.6.1 HF3, allows local administrator users to potentially disable some McAfee processes by manipulating the MA directory	https://kc.mcafee.com/corporate/index?page=content&id=SB10	A-MCA-AGEN-130819/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			control and placing a carefully constructed file in the MA directory. **CVE ID : CVE-2019-3592**	288	
data_loss_prevention_endpoint					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-07-2019	4.3	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in ePO extension in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.0 allows unauthenticated remote user to trigger specially crafted JavaScript to render in the ePO UI via a carefully crafted upload to a remote website which is correctly blocked by DLPe Web Protection. This would then render as an XSS when the DLP Admin viewed the event in the ePO UI. **CVE ID : CVE-2019-3591**	https://kc.mcafee.com/corporate/index?page=content&id=SB10289	A-MCA-DATA-130819/166
Improper Access Control	24-07-2019	4.6	Files or Directories Accessible to External Parties in McAfee Data Loss Prevention (DLPe) for Windows 11.x prior to 11.3.0 allows authenticated user to redirect DLPe log files to arbitrary locations via incorrect access control applied to the DLPe log folder allowing privileged users to create symbolic links. **CVE ID : CVE-2019-3622**	https://kc.mcafee.com/corporate/index?page=content&id=SB10290	A-MCA-DATA-130819/167
Metinfo					
metinfo					
Improper	19-07-2019	6.5	Metinfo 6.x allows SQL	N/A	A-MET-METI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			Injection via the id parameter in an admin/index.php?n=ui_set&m=admin&c=index&a=doget_text_content&table=lang&field=1 request. **CVE ID : CVE-2019-13969**		130819/168
Microsoft					
powershell_core					
N/A	19-07-2019	1.9	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1167**	N/A	A-MIC-POWE-130819/169
microstrategy					
microstrategy_web					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	In MicroStrategy Web before 10.4.6, there is stored XSS in metric due to insufficient input validation. **CVE ID : CVE-2019-12475**	N/A	A-MIC-MICR-130819/170
Modx					
modx_revolution					
Unrestricted Upload of File with Dangerous	23-07-2019	5	MODX Revolution Gallery 1.7.0 is affected by: CWE-434: Unrestricted Upload of File with Dangerous Type. The	N/A	A-MOD-MODX-130819/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			impact is: Creating file with custom a filename and content. The component is: Filtering user parameters before passing them into phpthumb class. The attack vector is: web request via /assets/components/gallery/connector.php. **CVE ID : CVE-2019-1010123**		
Moinejf					
abcm2ps					
Improper Access Control	18-07-2019	4.3	moinejf abcm2ps 8.13.20 is affected by: Incorrect Access Control. The impact is: Allows attackers to cause a denial of service attack via a crafted file. The component is: front.c, function txt_add. The fixed version is: after commit commit 08aef597656d065e86075f3d53fda89765845eae. **CVE ID : CVE-2019-1010069**	N/A	A-MOI-ABCM-130819/172
momo_project					
momo					
N/A	22-07-2019	4	The Momo application 2.1.9 for Android stores confidential information insecurely on the system (i.e., in cleartext), which allows a non-root user to find out the username/password of a valid user and a user's access token via Logcat. **CVE ID : CVE-2019-13099**	N/A	A-MOM-MOMO-130819/173
Mozilla					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
firefox					
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11691**	N/A	A-MOZ-FIRE-130819/174
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11692**	N/A	A-MOZ-FIRE-130819/175
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11693**	N/A	A-MOZ-FIRE-130819/176
Informatio	23-07-2019	5	A vulnerability exists in the	N/A	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11694**		130819/177
Improper Input Validation	23-07-2019	4.3	A custom cursor defined by scripting on a site can position itself over the addressbar to spoof the actual cursor when it should not be allowed outside of the primary web content area. This could be used by a malicious site to trick users into clicking on permission prompts, doorhanger notifications, or other buttons inadvertently if the location is spoofed over the user interface. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11695**	N/A	A-MOZ-FIRE-130819/178
Improper Input Validation	23-07-2019	6.8	Files with the .JNLP extension used for "Java web start" applications are not treated as executable content for download prompts even though they can be executed if Java is installed on the local system. This could allow users	N/A	A-MOZ-FIRE-130819/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to mistakenly launch an executable binary locally. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11696**		
Improper Input Validation	23-07-2019	4.3	If the ALT and "a" keys are pressed when users receive an extension installation prompt, the extension will be installed without the install prompt delay that keeps the prompt visible in order for users to accept or decline the installation. A malicious web page could use this with spoofing on the page to trick users into installing a malicious extension. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11697**	N/A	A-MOZ-FIRE-130819/180
Improper Input Validation	23-07-2019	5	If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11698**	N/A	A-MOZ-FIRE-130819/181
Improper	23-07-2019	4.3	A malicious page can briefly	N/A	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			cause the wrong name to be highlighted as the domain name in the addressbar during page navigations. This could result in user confusion of which site is currently loaded for spoofing attacks. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11699**		130819/182
Information Exposure	23-07-2019	4.3	A hyperlink using the res: protocol can be used to open local files at a known location in Internet Explorer if a user approves execution when prompted. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11700**	N/A	A-MOZ-FIRE-130819/183
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	The default webcal: protocol handler will load a web site vulnerable to cross-site scripting (XSS) attacks. This default was left in place as a legacy feature and has now been removed. *Note: this issue only affects users with an account on the vulnerable service. Other users are unaffected.*. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-11701**	N/A	A-MOZ-FIRE-130819/184
Information Exposure	23-07-2019	4.3	A hyperlink using protocols associated with Internet Explorer, such as IE.HTTP:, can be used to open local files at a known location with Internet	N/A	A-MOZ-FIRE-130819/185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Explorer if a user approves execution when prompted. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 67.0.2. **CVE ID : CVE-2019-11702**		
Incorrect Type Conversion or Cast	23-07-2019	7.5	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11707**	N/A	A-MOZ-FIRE-130819/186
Improper Input Validation	23-07-2019	10	Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11708**	N/A	A-MOZ-FIRE-130819/187
Improper Restriction	23-07-2019	7.5	Mozilla developers and community members reported	N/A	A-MOZ-FIRE-130819/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11709**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11710**	N/A	A-MOZ-FIRE-130819/189
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE-130819/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11711		
Cross-Site Request Forgery (CSRF)	23-07-2019	6.8	POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect response can bypass CORS requirements. This can allow an attacker to perform Cross-Site Request Forgery (CSRF) attacks. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11712**	N/A	A-MOZ-FIRE-130819/191
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11713**	N/A	A-MOZ-FIRE-130819/192
Improper Input Validation	23-07-2019	7.5	Necko can access a child on the wrong thread during UDP connections, resulting in a potentially exploitable crash in some instances. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11714**	N/A	A-MOZ-FIRE-130819/193
Improper Neutralization of Input During Web Page Generation ('Cross-site	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and	N/A	A-MOZ-FIRE-130819/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Thunderbird < 60.8. **CVE ID : CVE-2019-11715**		
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11717**	N/A	A-MOZ-FIRE-130819/195
Out-of-bounds Read	23-07-2019	5	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11719**	N/A	A-MOZ-FIRE-130819/196
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	Some unicode characters are incorrectly treated as whitespace during the parsing of web content instead of triggering parsing errors. This allows malicious code to then be processed, evading cross-site scripting (XSS) filtering. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11720**	N/A	A-MOZ-FIRE-130819/197
Improper Input	23-07-2019	4.3	The unicode latin 'kra' character can be used to spoof a standard 'k' character in the	N/A	A-MOZ-FIRE-130819/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			addressbar. This allows for domain spoofing attacks as do not display as punycode text, allowing for user confusion. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11721**		
Information Exposure	23-07-2019	5	A vulnerability exists during the installation of add-ons where the initial fetch ignored the origin attributes of the browsing context. This could leak cookies in private browsing mode or across different "containers" for people who use the Firefox Multi-Account Containers Web Extension. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11723**	N/A	A-MOZ-FIRE-130819/199
Improper Input Validation	23-07-2019	4	When a user navigates to site marked as unsafe by the Safebrowsing API, warning messages are displayed and navigation is interrupted but resources from the same site loaded through websockets are not blocked, leading to the loading of unsafe resources and bypassing safebrowsing protections. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11725**	N/A	A-MOZ-FIRE-130819/200
Improper Certificate Validation	23-07-2019	5	A vulnerability exists where it possible to force Network Security Services (NSS) to sign CertificateVerify with PKCS#1 v1.5 signatures when those are the only ones advertised by	N/A	A-MOZ-FIRE-130819/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server in CertificateRequest in TLS 1.3. PKCS#1 v1.5 signatures should not be used for TLS 1.3 messages. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11727**		
Improper Input Validation	23-07-2019	4.3	The HTTP Alternative Services header, Alt-Svc, can be used by a malicious site to scan all TCP ports of any host that the accessible to a user when web content is loaded. This vulnerability affects Firefox < 68. **CVE ID : CVE-2019-11728**	N/A	A-MOZ-FIRE-130819/202
Improper Input Validation	23-07-2019	5	Empty or malformed p256-ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11729**	N/A	A-MOZ-FIRE-130819/203
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.	N/A	A-MOZ-FIRE-130819/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9800		
N/A	23-07-2019	5.1	As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-9811**	N/A	A-MOZ-FIRE-130819/205
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-9814**	N/A	A-MOZ-FIRE-130819/206
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	23-07-2019	6.8	If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of this	N/A	A-MOZ-FIRE-130819/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			change.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9815**		
Incorrect Type Conversion or Cast	23-07-2019	4.3	A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. *Note: this vulnerability has only been demonstrated with UnboxedObjects, which are disabled by default on all supported releases.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9816**	N/A	A-MOZ-FIRE-130819/208
Origin Validation Error	23-07-2019	5	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9817**	N/A	A-MOZ-FIRE-130819/209
Improper Input Validation	23-07-2019	7.5	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This vulnerability affects	N/A	A-MOZ-FIRE-130819/210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9819**		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9820**	N/A	A-MOZ-FIRE-130819/211
Use After Free	23-07-2019	6.8	A use-after-free vulnerability can occur in AssertWorkerThread due to a race condition with shared workers. This results in a potentially exploitable crash. This vulnerability affects Firefox < 67. **CVE ID : CVE-2019-9821**	N/A	A-MOZ-FIRE-130819/212
firefox_esr					
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11691**	N/A	A-MOZ-FIRE-130819/213
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in	N/A	A-MOZ-FIRE-130819/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11692**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11693**	N/A	A-MOZ-FIRE-130819/215
Informatio n Exposure	23-07-2019	5	A vulnerability exists in the Windows sandbox where an uninitialized value in memory can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11694**	N/A	A-MOZ-FIRE-130819/216
Improper	23-07-2019	5	If a crafted hyperlink is	N/A	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11698**		130819/217
Incorrect Type Conversion or Cast	23-07-2019	7.5	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11707**	N/A	A-MOZ-FIRE-130819/218
Improper Input Validation	23-07-2019	10	Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's	N/A	A-MOZ-FIRE-130819/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11708**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11709**	N/A	A-MOZ-FIRE-130819/220
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11711**	N/A	A-MOZ-FIRE-130819/221
Cross-Site Request Forgery	23-07-2019	6.8	POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect	N/A	A-MOZ-FIRE-130819/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			response can bypass CORS requirements. This can allow an attacker to perform Cross-Site Request Forgery (CSRF) attacks. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11712**		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11713**	N/A	A-MOZ-FIRE-130819/223
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11715**	N/A	A-MOZ-FIRE-130819/224
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.	N/A	A-MOZ-FIRE-130819/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-11717		
Out-of-bounds Read	23-07-2019	5	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11719**	N/A	A-MOZ-FIRE-130819/226
Improper Input Validation	23-07-2019	5	Empty or malformed p256-ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11729**	N/A	A-MOZ-FIRE-130819/227
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9800**	N/A	A-MOZ-FIRE-130819/228
N/A	23-07-2019	5.1	As part of a winning Pwn2Own entry, a researcher	N/A	A-MOZ-FIRE-130819/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-9811**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	23-07-2019	6.8	If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in order to take advantage of this change.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9815**	N/A	A-MOZ-FIRE-130819/230
Incorrect Type Conversion or Cast	23-07-2019	4.3	A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. *Note: this vulnerability has only been demonstrated with UnboxedObjects, which are	N/A	A-MOZ-FIRE-130819/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disabled by default on all supported releases.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9816**		
Origin Validation Error	23-07-2019	5	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9817**	N/A	A-MOZ-FIRE-130819/232
Improper Input Validation	23-07-2019	7.5	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9819**	N/A	A-MOZ-FIRE-130819/233
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9820**	N/A	A-MOZ-FIRE-130819/234
thunderbird					
Use After	23-07-2019	7.5	A use-after-free vulnerability	N/A	A-MOZ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11691**		THUN-130819/235
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11692**	N/A	A-MOZ-THUN-130819/236
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11693**	N/A	A-MOZ-THUN-130819/237
Information Exposure	23-07-2019	5	A vulnerability exists in the Windows sandbox where an uninitialized value in memory	N/A	A-MOZ-THUN-130819/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be leaked to a renderer from a broker when making a call to access an otherwise unavailable file. This results in the potential leaking of information stored at that memory location. *Note: this issue only occurs on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11694**		
Improper Input Validation	23-07-2019	5	If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-11698**	N/A	A-MOZ-THUN-130819/239
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in parser_get_next_char when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1.	N/A	A-MOZ-THUN-130819/240

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
			CVE ID : CVE-2019-11703		
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in icalmemory_strdup_and_dequote when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1. **CVE ID : CVE-2019-11704**	N/A	A-MOZ-THUN-130819/241
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	A flaw in Thunderbird's implementation of iCal causes a stack buffer overflow in icalrecur_add_bydayrules when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1. **CVE ID : CVE-2019-11705**	N/A	A-MOZ-THUN-130819/242
Incorrect Type Conversion or Cast	23-07-2019	5	A flaw in Thunderbird's implementation of iCal causes a type confusion in icaltimezone_get_vtimezone_properties when processing certain email messages, resulting in a crash. This vulnerability affects Thunderbird < 60.7.1. **CVE ID : CVE-2019-11706**	N/A	A-MOZ-THUN-130819/243
Incorrect Type Conversion or Cast	23-07-2019	7.5	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in Array.pop. This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects	N/A	A-MOZ-THUN-130819/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11707**		
Improper Input Validation	23-07-2019	10	Insufficient vetting of parameters passed with the Prompt:Open IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2. **CVE ID : CVE-2019-11708**	N/A	A-MOZ-THUN-130819/245
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11709**	N/A	A-MOZ-THUN-130819/246
Improper Input Validation	23-07-2019	6.8	When an inner window is reused, it does not consider the use of document.domain for cross-origin protections. If	N/A	A-MOZ-THUN-130819/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pages on different subdomains ever cooperatively use document.domain, then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use document.domain to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11711**		
Cross-Site Request Forgery (CSRF)	23-07-2019	6.8	POST requests made by NPAPI plugins, such as Flash, that receive a status 308 redirect response can bypass CORS requirements. This can allow an attacker to perform Cross-Site Request Forgery (CSRF) attacks. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11712**	N/A	A-MOZ-THUN-130819/248
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11713**	N/A	A-MOZ-THUN-130819/249
Improper Neutralization of Input	23-07-2019	4.3	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead	N/A	A-MOZ-THUN-130819/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11715**		
Improper Input Validation	23-07-2019	5	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URIs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11717**	N/A	A-MOZ-THUN-130819/251
Out-of-bounds Read	23-07-2019	5	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11719**	N/A	A-MOZ-THUN-130819/252
Improper Input Validation	23-07-2019	5	Empty or malformed p256-ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-11729**	N/A	A-MOZ-THUN-130819/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-07-2019	7.5	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9800**	N/A	A-MOZ-THUN-130819/254
N/A	23-07-2019	5.1	As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8. **CVE ID : CVE-2019-9811**	N/A	A-MOZ-THUN-130819/255
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	23-07-2019	6.8	If hyperthreading is not disabled, a timing attack vulnerability exists, similar to previous Spectre attacks. Apple has shipped macOS 10.14.5 with an option to disable hyperthreading in applications running untrusted code in a thread through a new sysctl. Firefox now makes use of it on the main thread and any worker threads. *Note: users need to update to macOS 10.14.5 in	N/A	A-MOZ-THUN-130819/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			order to take advantage of this change.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9815**		
Incorrect Type Conversion or Cast	23-07-2019	4.3	A possible vulnerability exists where type confusion can occur when manipulating JavaScript objects in object groups, allowing for the bypassing of security checks within these groups. *Note: this vulnerability has only been demonstrated with UnboxedObjects, which are disabled by default on all supported releases.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9816**	N/A	A-MOZ-THUN-130819/257
Origin Validation Error	23-07-2019	5	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9817**	N/A	A-MOZ-THUN-130819/258
Improper Input Validation	23-07-2019	7.5	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This	N/A	A-MOZ-THUN-130819/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9819**		
Use After Free	23-07-2019	7.5	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7. **CVE ID : CVE-2019-9820**	N/A	A-MOZ-THUN-130819/260
mpg321_project					
mpg321					
Out-of-bounds Write	24-07-2019	4.3	The scan() function in mad.c in mpg321 0.3.2 allows remote attackers to trigger an out-of-bounds write via a zero bitrate in an MP3 file. **CVE ID : CVE-2019-14247**	N/A	A-MPG-MPG3-130819/261
myt_project					
myt					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	In MyT 1.5.1, the User[username] parameter has XSS. **CVE ID : CVE-2019-13346**	N/A	A-MYT-MYT-130819/262
nasa					
cfitsio					
Improper Restriction of	16-07-2019	7.5	NASA CFITSIO prior to 3.43 is affected by: Buffer Overflow. The impact is: arbitrary code	N/A	A-NAS-CFIT-130819/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			execution. The component is: over 40 source code files were changed. The attack vector is: remote unauthenticated attacker. The fixed version is: 3.43. NOTE: this CVE refers to the issues not covered by CVE-2018-3846, CVE-2018-3847, CVE-2018-3848, and CVE-2018-3849. One example is ftp_status in drvrnet.c mishandling a long string beginning with a '4' character. **CVE ID : CVE-2019-1010060**		
nevma					
adaptive_images					
Information Exposure	21-07-2019	5	A Local File Inclusion vulnerability in the Nevma Adaptive Images plugin before 0.6.67 for WordPress allows remote attackers to retrieve arbitrary files via the $REQUEST['adaptive-images-settings']['source_file'] parameter in adaptive-images-script.php. **CVE ID : CVE-2019-14205**	N/A	A-NEV-ADAP-130819/264
Improper Input Validation	21-07-2019	6.4	An Arbitrary File Deletion vulnerability in the Nevma Adaptive Images plugin before 0.6.67 for WordPress allows remote attackers to delete arbitrary files via the $REQUEST['adaptive-images-settings'] parameter in adaptive-images-script.php. **CVE ID : CVE-2019-14206**	N/A	A-NEV-ADAP-130819/265
nfdump_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nfdump					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	6.8	nfdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nffile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit 9f0fe9563366f62a71d34c92229da3432ec5cf0e. **CVE ID : CVE-2019-1010057**	N/A	A-NFD-NFDU-130819/266
Nginx					
njs					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	4.3	njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in nxt/nxt_sprintf.c during error handling, as demonstrated by an njs_regexp_literal call that leads to an njs_parser_lexer_error call and then an njs_parser_scope_error call. **CVE ID : CVE-2019-13617**	N/A	A-NGI-NJS-130819/267
norton					
password_manager					
Information Exposure	16-07-2019	1.7	Norton Password Manager, prior to 6.3.0.2082, may be susceptible to an address spoofing issue. This type of issue may allow an attacker to disguise their origin IP address	https://support.symantec.com/us/en/article.SYMSA1483.html	A-NOR-PASS-130819/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in order to obfuscate the source of network traffic. **CVE ID : CVE-2019-9700**		
NSA					
ghidra					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-07-2019	6.8	In NSA Ghidra through 9.0.4, path traversal can occur in RestoreTask.java (from the package ghidra.app.plugin.core.archive) via an archive with an executable file that has an initial ../ in its filename. This allows attackers to overwrite arbitrary files in scenarios where an intermediate analysis result is archived for sharing with other persons. To achieve arbitrary code execution, one approach is to overwrite some critical Ghidra modules, e.g., the decompile module. **CVE ID : CVE-2019-13623**	N/A	A-NSA-GHID-130819/269
Improper Restriction of XML External Entity Reference ('XXE')	16-07-2019	9.4	NSA Ghidra before 9.0.1 allows XXE when a project is opened or restored, or a tool is imported, as demonstrated by a project.prp file. **CVE ID : CVE-2019-13625**	N/A	A-NSA-GHID-130819/270
Offis					
dcmtk					
Improper Restriction of Operations within the	22-07-2019	7.5	OFFIS.de DCMTK 3.6.3 and below is affected by: Buffer Overflow. The impact is: Possible code execution and confirmed Denial of Service.	N/A	A-OFF-DCMT-130819/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			The component is: DcmRLEDecoder::decompress() (file dcrledec.h, line 122). The attack vector is: Many scenarios of DICOM file processing (e.g. DICOM to image conversion). The fixed version is: 3.6.4, after commit 40917614e. **CVE ID : CVE-2019-1010228**		
oisf					
suricata					
Improper Input Validation	18-07-2019	5	Open Information Security Foundation Suricata prior to version 4.1.2 is affected by: Denial of Service - DNS detection bypass. The impact is: An attacker can evade a signature detection with a specialy formed network packet. The component is: app-layer-detect-proto.c, decode.c, decode-teredo.c and decode-ipv6.c (https://github.com/OISF/suricata/pull/3590/commits/11f3659f64a4e42e90cb3c09fcef66894205aefe, https://github.com/OISF/suricata/pull/3590/commits/8357ef3f8ffc7d99ef6571350724160de356158b). The attack vector is: An attacker can trigger the vulnerability by sending a specifically crafted network request. The fixed version is: 4.1.2. **CVE ID : CVE-2019-1010251**	N/A	A-OIS-SURI-130819/272
onionbuzz					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
onionbuzz					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-07-2019	7.5	An issue was discovered in the Viral Quiz Maker - OnionBuzz plugin before 1.2.7 for WordPress. One could exploit the id parameter in the set_count ajax nopriv handler due to there being no sanitization prior to use in a SQL query in saveQuestionVote. This allows an unauthenticated/unprivileged user to perform a SQL injection attack capable of remote code execution and information disclosure. **CVE ID : CVE-2019-14230**	N/A	A-ONI-ONIO-130819/273
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-07-2019	7.5	An issue was discovered in the Viral Quiz Maker - OnionBuzz plugin before 1.2.2 for WordPress. One could exploit the points parameter in the ob_get_results ajax nopriv handler due to there being no sanitization prior to use in a SQL query in getResultByPointsTrivia. This allows an unauthenticated/unprivileged user to perform a SQL injection attack capable of remote code execution and information disclosure. **CVE ID : CVE-2019-14231**	N/A	A-ONI-ONIO-130819/274
onosproject					
onos					
N/A	16-07-2019	10	In ONOS 1.15.0, apps/yang/web/src/main/jav	N/A	A-ONO-ONOS-130819/275

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
			a/org/onosproject/yang/web/YangWebResource.java mishandles backquote characters within strings that can be used in a shell command. **CVE ID : CVE-2019-13624**		
opensns					
opensns					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	25-07-2019	6.5	OpenSNS v6.1.0 allows SQL Injection via the index.php?s=/ucenter/Config/uid parameter because of the getNeedQueryData function in Application/Common/Model/UserModel.class.php. **CVE ID : CVE-2019-14266**	N/A	A-OPE-OPEN-130819/276
Oracle					
retail_xstore_office					
Improper Access Control	23-07-2019	6.4	Vulnerability in the Oracle Retail Xstore Office component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 7.0 and 7.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Office. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Office accessible data as well as unauthorized	N/A	A-ORA-RETA-130819/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update, insert or delete access to some of Oracle Retail Xstore Office accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2561**		
bi_publisher					
Improper Access Control	23-07-2019	6.4	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-BI_P-130819/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2767**		
Information Exposure	23-07-2019	5	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2768**	N/A	A-ORA-BI_P-130819/279
Improper Access Control	23-07-2019	6	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher	N/A	A-ORA-BI_P-130819/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of BI Publisher (formerly XML Publisher). CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:H/A:L). **CVE ID : CVE-2019-2771**		
solaris					
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Automount). Supported versions that are affected are 11.4 and 10. Difficult to exploit vulnerability allows unauthenticated attacker with	N/A	A-ORA-SOLA-130819/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network access via NFS to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Solaris accessible data as well as unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2787**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Solaris component of Oracle Sun Systems Products Suite (subcomponent: Open Fabrics Tools). The supported version that is affected is 11.4. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Solaris executes to compromise Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Solaris accessible data and unauthorized ability to cause a hang or frequently repeatable	N/A	A-ORA-SOLA-130819/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of Solaris. CVSS 3.0 Base Score 6.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H). **CVE ID : CVE-2019-2788**		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Common Desktop Environment). The supported version that is affected is 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2832**	N/A	A-ORA-SOLA-130819/283
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11.4. Easily exploitable vulnerability	N/A	A-ORA-SOLA-130819/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows unauthenticated attacker with network access via NFS to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data. CVSS 3.0 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2838**		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: LDAP Client Tools). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2844**	N/A	A-ORA-SOLA-130819/285
Improper	23-07-2019	6.9	Vulnerability in the Oracle	N/A	A-ORA-SOLA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Solaris component of Oracle Sun Systems Products Suite (subcomponent: Filesystem). Supported versions that are affected are 11.4 and 10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2804**		130819/286
Improper Access Control	23-07-2019	3.3	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Zones). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	N/A	A-ORA-SOLA-130819/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of Oracle Solaris accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2807**		
Improper Access Control	23-07-2019	4.4	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Gnuplot). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Solaris. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2820**	N/A	A-ORA-SOLA-130819/288
demantra_demand_management					
Improper Access	23-07-2019	5	Vulnerability in the Oracle Demantra Demand	N/A	A-ORA-DEMA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Management component of Oracle Supply Chain Products Suite (subcomponent: Product Security). The supported version that is affected is 7.3.1.5.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Demantra Demand Management accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2732**		130819/289
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle Demantra Demand Management component of Oracle Supply Chain Products Suite (subcomponent: Product Security). The supported version that is affected is 7.3.1.5.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Demantra Demand Management. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Demantra Demand Management accessible data.	N/A	A-ORA-DEMA-130819/290

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
			CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2733**		
hyperion_workspace					
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle Hyperion Workspace component of Oracle Hyperion (subcomponent: UI and Visualization). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Workspace. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion Workspace accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2735**	N/A	A-ORA-HYPE-130819/291
flexcube_investor_servicing					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported	N/A	A-ORA-FLEX-130819/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Investor Servicing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2736**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable	N/A	A-ORA-FLEX-130819/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Investor Servicing accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2019-2841**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE	N/A	A-ORA-FLEX-130819/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Investor Servicing accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2843**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Investor Servicing. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	N/A	A-ORA-FLEX-130819/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2845		
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Investor Servicing. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2846**	N/A	A-ORA-FLEX-130819/296
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Investor Servicing component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1, 12.0.3, 12.0.4, 12.1.0, 12.3.0, 12.4.0, 14.0.0 and 14.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to	N/A	A-ORA-FLEX-130819/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromise Oracle FLEXCUBE Investor Servicing. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Investor Servicing accessible data. CVSS 3.0 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2847**		
flexcube_universal_banking					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle FLEXCUBE Universal Banking, attacks may significantly impact additional products.	N/A	A-ORA-FLEX-130819/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2744**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-FLEX-130819/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2790**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle FLEXCUBE Universal Banking. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2793**	N/A	A-ORA-FLEX-130819/300
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0	N/A	A-ORA-FLEX-130819/301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 14.0.0-14.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2794**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.1.0-12.4.0 and 14.0.0-14.2.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/U	N/A	A-ORA-FLEX-130819/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2839**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 5.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2840**	N/A	A-ORA-FLEX-130819/303
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle FLEXCUBE Universal Banking component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 12.0.1-12.0.3, 12.1.0-12.4.0 and 14.0.0-14.2.0. Easily	N/A	A-ORA-FLEX-130819/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle FLEXCUBE Universal Banking. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle FLEXCUBE Universal Banking accessible data as well as unauthorized access to critical data or complete access to all Oracle FLEXCUBE Universal Banking accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2019-2754**		
micros_retail-j					
Improper Access Control	23-07-2019	7.5	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Internal Operations). Supported versions that are affected are 12.1.0, 12.1.1, 12.1.2 and 13.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data as well	N/A	A-ORA-MICR-130819/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as unauthorized update, insert or delete access to some of MICROS Retail-J accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MICROS Retail-J. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L). **CVE ID : CVE-2019-2750**		
berkeley_db					
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2760**	N/A	A-ORA-BERK-130819/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2868**	N/A	A-ORA-BERK-130819/307
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this	N/A	A-ORA-BERK-130819/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2869**		
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and 12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2870**	N/A	A-ORA-BERK-130819/309
Improper Access Control	23-07-2019	3.7	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are 12.1.6.1.23, 12.1.6.1.26, 12.1.6.1.29, 12.1.6.1.36, 12.1.6.2.23 and	N/A	A-ORA-BERK-130819/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			12.1.6.2.32. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2871**		
food_and_beverage_applications					
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle Hospitality Simphony component of Oracle Food and Beverage Applications. The supported version that is affected is 18.2.1. Easily exploitable vulnerability allows low privileged attacker having Import/Export privilege with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	N/A	A-ORA-FOOD-130819/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 7.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-2833**		
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Hospitality Simphony component of Oracle Food and Beverage Applications. The supported version that is affected is 18.2.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Simphony accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2836**	N/A	A-ORA-FOOD-130819/312
Improper Access Control	23-07-2019	6.4	Vulnerability in the Oracle Hospitality Gift and Loyalty component of Oracle Food and Beverage Applications. Supported versions that are affected are 9.0.0 and 9.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Gift and	N/A	A-ORA-FOOD-130819/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Loyalty. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Gift and Loyalty accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Gift and Loyalty accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2763**		
hyperion_planning					
Improper Access Control	23-07-2019	3.5	Vulnerability in the Oracle Hyperion Planning component of Oracle Hyperion (subcomponent: Smart View). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hyperion Planning accessible data. CVSS 3.0 Base Score 4.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	A-ORA-HYPE-130819/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2770**		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle Hyperion Planning component of Oracle Hyperion (subcomponent: Security). The supported version that is affected is 11.1.2.4. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Hyperion Planning. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hyperion Planning accessible data. CVSS 3.0 Base Score 4.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N). **CVE ID : CVE-2019-2861**	N/A	A-ORA-HYPE-130819/315
payments					
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Payments component of Oracle E-Business Suite (subcomponent: File Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments.	N/A	A-ORA-PAYM-130819/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Payments accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2782**		
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Payments component of Oracle E-Business Suite (subcomponent: File Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. While the vulnerability is in Oracle Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Payments accessible data. CVSS 3.0 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2019-2783**	N/A	A-ORA-PAYM-130819/317
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle Payments component of Oracle E-Business Suite (subcomponent: File	N/A	A-ORA-PAYM-130819/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. While the vulnerability is in Oracle Payments, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Payments accessible data. CVSS 3.0 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N). **CVE ID : CVE-2019-2773**		
Improper Access Control	23-07-2019	6.4	Vulnerability in the Oracle Payments component of Oracle E-Business Suite (subcomponent: File Transmission). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Payments. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Payments accessible data and unauthorized ability to cause a hang or frequently repeatable	N/A	A-ORA-PAYM-130819/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of Oracle Payments. CVSS 3.0 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2019-2775**		
siebel_core_-_server_framework					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Siebel Core - Server Framework component of Oracle Siebel CRM (subcomponent: Search). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Core - Server Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel Core - Server Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server Framework accessible data as well as unauthorized read access to a subset of Siebel Core - Server Framework accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector:	N/A	A-ORA-SIEB-130819/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2777**		
hospitality_suite8					
Information Exposure	23-07-2019	4	Vulnerability in the Oracle Hospitality Suite8 component of Oracle Hospitality Applications (subcomponent: XML Interface). Supported versions that are affected are 8.9.6, 8.10.2 and 8.11-8.14. Easily exploitable vulnerability allows low privileged attacker with network access via TCP/IP to compromise Oracle Hospitality Suite8. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Suite8 accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2781**	N/A	A-ORA-HOSP-130819/321
irecruitment					
Improper Access Control	23-07-2019	5	Vulnerability in the Oracle iRecruitment component of Oracle E-Business Suite (subcomponent: Password Reset). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	N/A	A-ORA-IREC-130819/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle iRecruitment. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle iRecruitment. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2809**		
graalvm					
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle GraalVM Enterprise Edition component of Oracle GraalVM (subcomponent: GraalVM). The supported version that is affected is 19.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	N/A	A-ORA-GRAA-130819/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2813		
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle GraalVM Enterprise Edition component of Oracle GraalVM (subcomponent: Java). The supported version that is affected is 19.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle GraalVM Enterprise Edition. CVSS 3.0 Base Score 6.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H). **CVE ID : CVE-2019-2862**	N/A	A-ORA-GRAA-130819/324
siebel_core_-_common_components					
Improper Access Control	23-07-2019	4.9	Vulnerability in the Siebel Core - Common Components component of Oracle Siebel CRM (subcomponent: Email). Supported versions that are affected are 19.0 and prior. Difficult to exploit	N/A	A-ORA-SIEB-130819/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel Core - Common Components. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Siebel Core - Common Components accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2779**		
agile_product_lifecycle_management					
Improper Access Control	23-07-2019	3.6	Vulnerability in the Oracle Agile PLM component of Oracle Supply Chain Products Suite (subcomponent: Folders, Files & Attachments). Supported versions that are affected are 9.3.3, 9.3.4, 9.3.5 and 9.3.6. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all	N/A	A-ORA-AGIL-130819/326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle Agile PLM accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Agile PLM. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:N/A:L). **CVE ID : CVE-2019-2817**		
financial_services_analytical_applications_infrastructure					
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle Financial Services Analytical Applications Infrastructure component of Oracle Financial Services Applications (subcomponent: Infrastructure). Supported versions that are affected are 8.0.5-8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financial Services Analytical Applications Infrastructure. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Financial Services Analytical Applications Infrastructure accessible data as well as unauthorized read access to a subset of Oracle Financial Services Analytical Applications Infrastructure accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and	N/A	A-ORA-FINA-130819/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2823**		
applications_manager					
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: Oracle Diagnostics Interfaces). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N). **CVE ID : CVE-2019-2825**	N/A	A-ORA-APPL-130819/328
field_service					
Improper	23-07-2019	6.8	Vulnerability in the Oracle	N/A	A-ORA-FIEL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Field Service component of Oracle E-Business Suite (subcomponent: Wireless). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Field Service, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle Field Service. CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2828**		130819/329
isupport					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle iSupport component of Oracle E-Business Suite (subcomponent: Service Requests). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupport. Successful	N/A	A-ORA-ISUP-130819/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupport, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iSupport accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupport accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2829**		
peoplesoft_enterprise_fin_project_costing					
Improper Access Control	23-07-2019	5.5	Vulnerability in the PeopleSoft Enterprise FIN Project Costing component of Oracle PeopleSoft Products (subcomponent: Projects). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Project Costing. While the vulnerability is in PeopleSoft Enterprise FIN Project Costing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA-PEOP-130819/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized update, insert or delete access to some of PeopleSoft Enterprise FIN Project Costing accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of PeopleSoft Enterprise FIN Project Costing. CVSS 3.0 Base Score 6.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:L). **CVE ID : CVE-2019-2831**		
siebel_ui_framework					
Improper Access Control	23-07-2019	4.9	Vulnerability in the Siebel UI Framework component of Oracle Siebel CRM (subcomponent: UIF Open UI). Supported versions that are affected are 19.0 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel UI Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Siebel UI Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel UI Framework accessible data as well as unauthorized read access to a subset of Siebel UI	N/A	A-ORA-SIEB-130819/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Framework accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2857**		
identity_manager					
Improper Access Control	23-07-2019	4	Vulnerability in the Oracle Identity Manager component of Oracle Fusion Middleware (subcomponent: Advanced Console). Supported versions that are affected are 11.1.2.3.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Identity Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Identity Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2858**	N/A	A-ORA-IDEN-130819/333
clusterware					
Improper Access Control	23-07-2019	6.8	Vulnerability in the Oracle Clusterware component of Oracle Support Tools (subcomponent: Trace File Analyzer (TFA) Collector). The supported version that is affected is 12.1.0.2.0. Difficult to exploit vulnerability allows	N/A	A-ORA-CLUS-130819/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker with network access via multiple protocols to compromise Oracle Clusterware. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Clusterware accessible data as well as unauthorized read access to a subset of Oracle Clusterware accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Clusterware. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2860**		
sun_zfs_storage_appliance_kit					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) component of Oracle Sun Systems Products Suite (subcomponent: HTTP data path subsystems). The supported version that is affected is 8.8.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Sun ZFS Storage Appliance Kit (AK). Successful attacks require human interaction from a person other than the attacker and while the	N/A	A-ORA-SUN_-130819/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is in Sun ZFS Storage Appliance Kit (AK), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Sun ZFS Storage Appliance Kit (AK) accessible data as well as unauthorized read access to a subset of Sun ZFS Storage Appliance Kit (AK) accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2878**		
http_server					
Improper Access Control	23-07-2019	4.3	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: OHS Config MBeans). Supported versions that are affected are 12.1.3.0.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle HTTP Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U	N/A	A-ORA-HTTP-130819/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2751**		
mysql					
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior and 5.7.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2730**	N/A	A-ORA-MYSQ-130819/337
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or	N/A	A-ORA-MYSQ-130819/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2731**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2737**	N/A	A-ORA-MYSQ-130819/339
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and	N/A	A-ORA-MYSQ-130819/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2738**		
Improper Access Control	23-07-2019	3.6	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability	N/A	A-ORA-MYSQ-130819/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2739**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2740**	N/A	A-ORA-MYSQ-130819/342
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	N/A	A-ORA-MYSQ-130819/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2741**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.12 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2743**	N/A	A-ORA-MYSQ-130819/344
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Data Dictionary). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability	N/A	A-ORA-MYSQ-130819/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2746**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2747**	N/A	A-ORA-MYSQ-130819/346
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent:	N/A	A-ORA-MYSQ-130819/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2778**		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Components / Services). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score	N/A	A-ORA-MYSQ-130819/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2780**		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2784**	N/A	A-ORA-MYSQ-130819/349
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized	N/A	A-ORA-MYSQ-130819/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2785**		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2789**	N/A	A-ORA-MYSQ-130819/351
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker	N/A	A-ORA-MYSQ-130819/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2791**		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2795**	N/A	A-ORA-MYSQ-130819/353
Improper	23-07-2019	4	Vulnerability in the MySQL	N/A	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2796**		130819/354
Improper Access Control	23-07-2019	2.3	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base	N/A	A-ORA-MYSQ-130819/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2797**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2798**	N/A	A-ORA-MYSQ-130819/356
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in	N/A	A-ORA-MYSQ-130819/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2800**		
Improper Input Validation	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2826**	N/A	A-ORA-MYSQ-130819/358
Improper Input Validation	23-07-2019	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are	N/A	A-ORA-MYSQ-130819/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2830**		
Improper Input Validation	23-07-2019	6.8	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2834**	N/A	A-ORA-MYSQ-130819/360
Improper	23-07-2019	4	Vulnerability in the MySQL	N/A	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2879**		130819/361
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	A-ORA-MYSQ-130819/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2752**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2755**	N/A	A-ORA-MYSQ-130819/363
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or	N/A	A-ORA-MYSQ-130819/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2757**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2758**	N/A	A-ORA-MYSQ-130819/365
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16	N/A	A-ORA-MYSQ-130819/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2774**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2801**	N/A	A-ORA-MYSQ-130819/367
Improper	23-07-2019	4	Vulnerability in the MySQL	N/A	A-ORA-MYSQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2802**		130819/368
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	A-ORA-MYSQ-130819/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2803**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2805**	N/A	A-ORA-MYSQ-130819/370
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	N/A	A-ORA-MYSQ-130819/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2808**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2810**	N/A	A-ORA-MYSQ-130819/372
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server.	N/A	A-ORA-MYSQ-130819/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2811**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2812**	N/A	A-ORA-MYSQ-130819/374
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows high	N/A	A-ORA-MYSQ-130819/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 2.2 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2814**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2815**	N/A	A-ORA-MYSQ-130819/376
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit).	N/A	A-ORA-MYSQ-130819/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2819**		
Improper Input Validation	23-07-2019	5.1	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell: Admin / InnoDB Cluster). Supported versions that are affected are 8.0.16 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in	N/A	A-ORA-MYSQ-130819/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			takeover of MySQL Server. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2822**		
jdk					
Improper Access Control	23-07-2019	1.9	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1	N/A	A-ORA-JDK-130819/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2745**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be	N/A	A-ORA-JDK-130819/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N). **CVE ID : CVE-2019-2786**		
Improper Access Control	23-07-2019	4.3	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is Java SE: 8u212. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS	N/A	A-ORA-JDK-130819/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2842**		
Improper Access Control	23-07-2019	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U	N/A	A-ORA-JDK-130819/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2762**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector:	N/A	A-ORA-JDK-130819/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2766**		
Improper Access Control	23-07-2019	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/U	N/A	A-ORA-JDK-130819/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2769**		
Improper Access Control	23-07-2019	5.8	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity	N/A	A-ORA-JDK-130819/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2816**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/U	N/A	A-ORA-JDK-130819/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2818**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).	N/A	A-ORA-JDK-130819/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2821		
jre					
Improper Access Control	23-07-2019	1.9	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2745**	N/A	A-ORA-JRE-130819/388
Improper Access	23-07-2019	2.6	Vulnerability in the Java SE, Java SE Embedded component	N/A	A-ORA-JRE-130819/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N). **CVE ID : CVE-2019-2786**		
Improper Access Control	23-07-2019	4.3	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is Java SE: 8u212. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2842**	N/A	A-ORA-JRE-130819/390
Improper Access	23-07-2019	5	Vulnerability in the Java SE, Java SE Embedded component	N/A	A-ORA-JRE-130819/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2762**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking).	N/A	A-ORA-JRE-130819/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2766**		
Improper Access	23-07-2019	5	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE	N/A	A-ORA-JRE-130819/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			(subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2769**		
Improper Access Control	23-07-2019	5.8	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are	N/A	A-ORA-JRE-130819/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2816**		
Improper Access	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security).	N/A	A-ORA-JRE-130819/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2818**		
Improper Access Control	23-07-2019	2.6	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit	N/A	A-ORA-JRE-130819/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2821**		
outside_in_technology					
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is	N/A	A-ORA-OUTS-130819/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2792**		
Improper Access	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion	N/A	A-ORA-OUTS-130819/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2835**		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	N/A	A-ORA-OUTS-130819/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2756**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score	N/A	A-ORA-OUTS-130819/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2759**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code,	N/A	A-ORA-OUTS-130819/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2764**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the	N/A	A-ORA-OUTS-130819/402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2852**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the	N/A	A-ORA-OUTS-130819/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2853**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a	N/A	A-ORA-OUTS-130819/404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2854**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of	N/A	A-ORA-OUTS-130819/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2855**		
vm_virtualbox					
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of	N/A	A-ORA-VM_V-130819/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). **CVE ID : CVE-2019-2848**		
Improper Access Control	23-07-2019	1.9	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 2.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2850**	N/A	A-ORA-VM_V-130819/407
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization	N/A	A-ORA-VM_V-130819/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2859**		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional	N/A	A-ORA-VM_V-130819/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N). **CVE ID : CVE-2019-2863**		
Improper Access Control	23-07-2019	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2864**	N/A	A-ORA-VM_V-130819/410
Improper Access Control	23-07-2019	4.4	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization	N/A	A-ORA-VM_V-130819/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2865**		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of	N/A	A-ORA-VM_V-130819/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2866**		
Improper Access Control	23-07-2019	4.6	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H). **CVE ID : CVE-2019-2867**	N/A	A-ORA-VM_V-130819/413
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core).	N/A	A-ORA-VM_V-130819/414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2873**		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector:	N/A	A-ORA-VM_V-130819/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2874**		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI :N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2875**	N/A	A-ORA-VM_V-130819/416
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM	N/A	A-ORA-VM_V-130819/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). **CVE ID : CVE-2019-2876**		
Improper Access Control	23-07-2019	2.1	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.32 and prior to 6.0.10. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2877**	N/A	A-ORA-VM_V-130819/418
database_server					
Improper Access	23-07-2019	4.9	Vulnerability in the Java VM component of Oracle Database Server. Supported versions	N/A	A-ORA-DATA-130819/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java VM accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java VM. CVSS 3.0 Base Score 6.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:H). **CVE ID : CVE-2019-2749**		
N/A	23-07-2019	5.5	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Any Index privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical	N/A	A-ORA-DATA-130819/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data or complete access to all Core RDBMS accessible data as well as unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2776**		
Improper Access Control	23-07-2019	6	Vulnerability in the Oracle ODBC Driver component of Oracle Database Server ***PRIVILEGE CANNOT BE NONE FOR AUTHENTICATED ATTACKS***. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Difficult to exploit vulnerability allows low privileged attacker having None privilege with network access via multiple protocols to compromise Oracle ODBC Driver. Successful attacks of this vulnerability can result in takeover of Oracle ODBC Driver. Note: The vulnerability affects Windows platforms only. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2799**	N/A	A-ORA-DATA-130819/421
N/A	23-07-2019	4.9	Vulnerability in the Application Express	N/A	A-ORA-DATA-130819/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component of Oracle Database Server. Supported versions that are affected are 5.1 and 18.2. Easily exploitable vulnerability allows low privileged attacker having Valid Account privilege with network access via HTTP to compromise Application Express. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Application Express, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Application Express accessible data as well as unauthorized read access to a subset of Application Express accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2484**		
Improper Access Control	23-07-2019	1.2	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Difficult to exploit vulnerability allows high privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes	N/A	A-ORA-DATA-130819/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Core RDBMS accessible data. CVSS 3.0 Base Score 4.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2569**		
Improper Access Control	23-07-2019	4.9	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Oracle Text. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Text accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Text. CVSS 3.0 Base Score 4.6 (Confidentiality and Availability impacts). CVSS Vector:	N/A	A-ORA-DATA-130819/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:L). **CVE ID : CVE-2019-2753**		
application_testing_suite					
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L). **CVE ID : CVE-2019-2727**	N/A	A-ORA-APPL-130819/425
business_intelligence_publisher					
Improper	23-07-2019	6.4	Vulnerability in the Oracle BI	N/A	A-ORA-BUSI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			Publisher component of Oracle Fusion Middleware (subcomponent: Web Service API). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data as well as unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2742**		130819/426
one-to-one_fulfillment					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise	N/A	A-ORA-ONE--130819/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2666**		
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is	N/A	A-ORA-ONE--130819/428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2668**		
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1 - 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	N/A	A-ORA-ONE--130819/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2672**		
application_object_library					
Improper Access Control	23-07-2019	4.3	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.8. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2761**	N/A	A-ORA-APPL-130819/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
crm_technical_foundation					
Improper Access Control	23-07-2019	5.8	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.3 and 12.2.3 - 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N). **CVE ID : CVE-2019-2837**	N/A	A-ORA-CRM_-130819/431
weblogic_server					
Improper	23-07-2019	5.5	Vulnerability in the Oracle	N/A	A-ORA-WEBL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2827**		130819/432
Improper Access Control	23-07-2019	5.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical	N/A	A-ORA-WEBL-130819/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N). **CVE ID : CVE-2019-2824**		
Improper Access Control	23-07-2019	7.5	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Application Container - JavaEE). Supported versions that are affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2019-2856**	N/A	A-ORA-WEBL-130819/434
peoplesoft_enterprise_peopletools					
Information Exposure	23-07-2019	4	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Pagelet Wizard). Supported versions	N/A	A-ORA-PEOP-130819/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). **CVE ID : CVE-2019-2599**		
Improper Access Control	23-07-2019	4.9	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all	N/A	A-ORA-PEOP-130819/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:H/A:N). **CVE ID : CVE-2019-2748**		
Improper Access Control	23-07-2019	5.8	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Activity Guide). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise	N/A	A-ORA-PEOP-130819/437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N). **CVE ID : CVE-2019-2772**		
enterprise_manager_ops_center					
Improper Access Control	23-07-2019	4	Vulnerability in the Enterprise Manager Ops Center component of Oracle Enterprise Manager Products Suite (subcomponent: Networking). Supported versions that are affected are 12.3.3 and 12.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Enterprise Manager Ops Center. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Ops Center accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N). **CVE ID : CVE-2019-2728**	N/A	A-ORA-ENTE-130819/438
otcms					
otcms					
Improper Neutralization of Input During	19-07-2019	4.3	OTCMS 3.81 allows XSS via the mode parameter in an apiRun.php?mudi=autoRun request.	N/A	A-OTC-OTCM-130819/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2019-13971**		
Ovidentia					
ovidentia					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	3.5	index.php in Ovidentia 8.4.3 has XSS via tg=groups, tg=maildoms&idx=create&userid=0&bgrp=y, tg=delegat, tg=site&idx=create, tg=site&item=4, tg=admdir&idx=mdb&id=1, tg=notes&idx=Create, tg=admfaqs&idx=Add, or tg=admoc&idx=addoc&item=. **CVE ID : CVE-2019-13977**	N/A	A-OVI-OVID-130819/440
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	6.5	Ovidentia 8.4.3 has SQL Injection via the id parameter in an index.php?tg=delegat&idx=mem request. **CVE ID : CVE-2019-13978**	N/A	A-OVI-OVID-130819/441
palletsprojects					
flask					
N/A	17-07-2019	5	The Pallets Project Flask before 1.0 is affected by: unexpected memory usage. The impact is: denial of service. The attack vector is: crafted encoded JSON data. The fixed version is: 1. **CVE ID : CVE-2019-1010083**	https://www.palletsprojects.com/blog/flask-1-0-released/	A-PAL-FLAS-130819/442
Pango					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pango					
Improper Restriction of Operations within the Bounds of a Memory Buffer	19-07-2019	7.5	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow can be used to get code execution. The component is: function name: pango_log2vis_get_embedding_levels, assignment of nchars and the loop condition. The attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize. **CVE ID : CVE-2019-1010238**	N/A	A-PAN-PANG-130819/443
phpcoo					
oecms					
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	OECMS v4.3.R60321 and v4.3 later is affected by: Cross Site Request Forgery (CSRF). The impact is: The victim clicks on adding an administrator account. The component is: admincp.php. The attack vector is: network connectivity. The fixed version is: v4.3. **CVE ID : CVE-2019-1010112**	N/A	A-PHP-OECM-130819/444
pivotal_software					
cloud_foundry_uaa					
Improper Input Validation	18-07-2019	4.3	Cloud Foundry UAA, versions prior to v73.4.0, does not set an X-FRAME-OPTIONS header on various endpoints. A remote user can perform clickjacking attacks on UAA's frontend sites. **CVE ID : CVE-2019-3794**	https://www.cloudfoundry.org/blog/cve-2019-3794	A-PIV-CLOU-130819/445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pluck-cms					
pluckcms					
Unrestricted Upload of File with Dangerous Type	16-07-2019	7.5	PluckCMS 4.7.4 and earlier is affected by: CWE-434 Unrestricted Upload of File with Dangerous Type. The impact is: get webshell. The component is: data/inc/images.php line36. The attack vector is: modify the MIME TYPE on HTTP request to upload a php file. The fixed version is: after commit 09f0ab871bf633973cfd9fc4fe59d4a912397cf8. **CVE ID : CVE-2019-1010062**	N/A	A-PLU-PLUC-130819/446
premiumsoftware					
cleditor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-07-2019	4.3	Premium Software CLEditor 1.4.5 and earlier is affected by: Cross Site Scripting (XSS). The impact is: An attacker might be able to inject arbitrary html and script code into the web site. The component is: jQuery plug-in. The attack vector is: the victim must open a crafted href attribute of a link (A) element. **CVE ID : CVE-2019-1010113**	N/A	A-PRE-CLED-130819/447
Proftpd					
proftpd					
Improper Access Control	19-07-2019	7.5	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure	N/A	A-PRO-PROF-130819/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without authentication, a related issue to CVE-2015-3306. **CVE ID : CVE-2019-12815**		
Qbittorrent					
qbittorrent					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	7.5	In qBittorrent before 4.1.7, the function Application::runExternalProgram() located in app/application.cpp allows command injection via shell metacharacters in the torrent name parameter or current tracker parameter, as demonstrated by remote command execution via a crafted name within an RSS feed. **CVE ID : CVE-2019-13640**	N/A	A-QBI-QBIT-130819/449
quake3e_project					
quake3e					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	7.5	Quake3e < 5ed740d is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Argument string creation. **CVE ID : CVE-2019-1010043**	N/A	A-QUA-QUAK-130819/450
rangerstudio					
directus_7_api					
Unrestricted Upload of File with Dangerous Type	19-07-2019	6.8	In Directus 7 API through 2.3.0, uploading of PHP files is blocked only when the Apache HTTP Server is used, leading to uploads/_/originals remote	N/A	A-RAN-DIRE-130819/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution with nginx. **CVE ID : CVE-2019-13980**		
Improper Input Validation	19-07-2019	5	In Directus 7 API through 2.3.0, remote attackers can read image files via a direct request for a filename under the uploads/_/originals/ directory. This is related to a configuration option in which the file collection can be non-public, but this option does not apply to the thumbnailer. **CVE ID : CVE-2019-13981**	N/A	A-RAN-DIRE-130819/452
directus_7					
Information Exposure	19-07-2019	5	interfaces/markdown/input.vue in Directus 7 Application before 7.7.0 does not sanitize Markdown text before rendering a preview. **CVE ID : CVE-2019-13982**	N/A	A-RAN-DIRE-130819/453
rdbrck					
shift					
Improper Authentication	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-12911**	https://support.tryshift.com/kb/article/206-shift-34-released-on-january-23-2019/	A-RDB-SHIF-130819/454
Untrusted Search Path	17-07-2019	2.1	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-12912**	https://support.tryshift.com/kb/article/206-shift-34-released-on-	A-RDB-SHIF-130819/455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				january-23-2019/	
N/A	17-07-2019	2.1	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-12913**	https://support.tryshift.com/kb/article/206-shift-34-released-on-january-23-2019/	A-RDB-SHIF-130819/456
Improper Authentication	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-12914**	https://support.tryshift.com/kb/article/206-shift-34-released-on-january-23-2019/	A-RDB-SHIF-130819/457
Information Exposure	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-8931**	https://support.tryshift.com/kb/article/206-shift-34-released-on-january-23-2019/	A-RDB-SHIF-130819/458
Improper Authentication	17-07-2019	5	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application. **CVE ID : CVE-2019-8932**	https://support.tryshift.com/kb/article/206-shift-34-released-on-january-23-2019/	A-RDB-SHIF-130819/459
Saltstack					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
salt_2019					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack/salt/blob/develop/salt/modules/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4. **CVE ID : CVE-2019-1010259**	N/A	A-SAL-SALT-130819/460
salt_2018					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack/salt/blob/develop/salt/modules/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4. **CVE ID : CVE-2019-1010259**	N/A	A-SAL-SALT-130819/461
scapy					
scapy					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	19-07-2019	5	scapy 2.4.0 is affected by: Denial of Service. The impact is: infinite loop, resource consumption and program unresponsive. The component is: _RADIUSAttrPacketListField.getfield(self..). The attack vector is: over the network or in a pcap. both work. **CVE ID : CVE-2019-1010142**	N/A	A-SCA-SCAP-130819/462
send-anywhere					
send_anywhere					
N/A	22-07-2019	4	The Send Anywhere application 9.4.18 for Android stores confidential information insecurely on the system (i.e., in cleartext), which allows a non-root user to find out the username/password of a valid user via /data/data/com.estmob.android.sendanywhere/shared_prefs/sendanywhere_device.xml. **CVE ID : CVE-2019-13100**	N/A	A-SEN-SEND-130819/463
sertek					
xpare					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-07-2019	10	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could access the backend database via SQL injection. **CVE ID : CVE-2019-13447**	N/A	A-SER-XPAR-130819/464
Improper	17-07-2019	4.3	An issue was discovered in	N/A	A-SER-XPAR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could exploit the vulnerable function in order to prepare an XSS payload to send to the product's clients. **CVE ID : CVE-2019-13448**		130819/465
servicestack					
servicestack					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	ServiceStack ServiceStack Framework 4.5.14 is affected by: Cross Site Scripting (XSS). The impact is: JavaScrpit is reflected in the server response, hence executed by the browser. The component is: the query used in the GET request is prone. The attack vector is: Since there is no server-side validation and If Browser encoding is bypassed, the victim is affected when opening a crafted URL. The fixed version is: 5.2.0. **CVE ID : CVE-2019-1010199**	N/A	A-SER-SERV-130819/466
Sitecore					
experience_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	3.5	In Sitecore 9.0 rev 171002, Persistent XSS exists in the Media Library and File Manager. An authenticated unprivileged user can modify the uploaded file extension parameter to inject arbitrary JavaScript. **CVE ID : CVE-2019-13493**	N/A	A-SIT-EXPE-130819/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sleuthkit					
the_sleuth_kit					
Integer Overflow or Wraparound	18-07-2019	4.3	The Sleuth Kit 4.6.0 and earlier is affected by: Integer Overflow. The impact is: Opening crafted disk image triggers crash in tsk/fs/hfs_dent.c:237. The component is: Overflow in fls tool used on HFS image. Bug is in tsk/fs/hfs.c file in function hfs_cat_traverse() in lines: 952, 1062. The attack vector is: Victim must open a crafted HFS filesystem image. **CVE ID : CVE-2019-1010065**	N/A	A-SLE-THE_-130819/468
Status					
react_native_desktop					
Improper Input Validation	23-07-2019	7.5	ubuntu-server.js in Status React Native Desktop before v0.57.8_mobile_ui allows Remote Code Execution. **CVE ID : CVE-2019-12164**	https://github.com/status-im/react-native-desktop/pull/475/commits/f6945f1e4b157c69e414cd94fe5cde1876aabcc1	A-STA-REAC-130819/469
Sweetscape					
010_editor					
Improper Input Validation	22-07-2019	5.8	In SweetScape 010 Editor 9.0.1, improper validation of arguments in the internal implementation of the Memcpy function (provided by	N/A	A-SWE-010_-130819/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the scripting engine) allows an attacker to overwrite arbitrary memory, which could lead to code execution. **CVE ID : CVE-2019-12551**		
Integer Overflow or Wraparound	22-07-2019	4.3	In SweetScape 010 Editor 9.0.1, an integer overflow during the initialization of variables could allow an attacker to cause a denial of service. **CVE ID : CVE-2019-12552**	N/A	A-SWE-010_-130819/471
syguestbook_a5_project					
syguestbook_a5					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-07-2019	3.5	SyGuestBook A5 Version 1.2 allows stored XSS because the isValidData function in include/functions.php does not properly block XSS payloads, as demonstrated by a crafted use of the onerror attribute of an IMG element. **CVE ID : CVE-2019-13948**	N/A	A-SYG-SYGU-130819/472
Cross-Site Request Forgery (CSRF)	18-07-2019	6.8	SyGuestBook A5 Version 1.2 has no CSRF protection mechanism, as demonstrated by CSRF for an index.php?c=Administrator&a=update admin password change. **CVE ID : CVE-2019-13949**	N/A	A-SYG-SYGU-130819/473
Improper Neutralization of Input During Web Page Generation	18-07-2019	3.5	index.php?c=admin&a=index in SyGuestBook A5 Version 1.2 has stored XSS via a reply to a comment. **CVE ID : CVE-2019-13950**	N/A	A-SYG-SYGU-130819/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')					
Tcpdump					
tcpdump					
Out-of-bounds Read	22-07-2019	4.3	tcpdump.org tcpdump 4.9.2 is affected by: CWE-126: Buffer Over-read. The impact is: May expose Saved Frame Pointer, Return Address etc. on stack. The component is: line 234: "ND_PRINT((ndo, "%s", buf));", in function named "print_prefix", in "print-hncp.c". The attack vector is: The victim must open a specially crafted pcap file. **CVE ID : CVE-2019-1010220**	N/A	A-TCP-TCPD-130819/475
techytalk					
quick_chat					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	TechyTalk Quick Chat WordPress Plugin All up to the latest is affected by: SQL Injection. The impact is: Access to the database. The component is: like_escape is used in Quick-chat.php line 399. The attack vector is: Crafted ajax request. **CVE ID : CVE-2019-1010104**	N/A	A-TEC-QUIC-130819/476
temenos					
cwx					
Improper Access Control	17-07-2019	5	Temenos CWX version 8.9 has an Broken Access Control vulnerability in the module /CWX/Employee/EmployeeEdit2.aspx, leading to the viewing of user information.	N/A	A-TEM-CWX-130819/477

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13403		
timesheet_next_gen_project					
timesheet_next_gen					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	Timesheet Next Gen 1.5.3 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via a "redirect" parameter. The component is: Web login form: login.php, lines 40 and 54. The attack vector is: reflected XSS, victim may click the malicious url. **CVE ID : CVE-2019-1010287**	N/A	A-TIM-TIME-130819/478
tiny.cloud					
tinymce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-07-2019	4.3	tinymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab. **CVE ID : CVE-2019-1010091**	N/A	A-TIN-TINY-130819/479
tronlink					
wallet					
N/A	22-07-2019	5	TronLink Wallet 2.2.0 stores user wallet keystore in plaintext and places them in insecure storage. An attacker can read and reuse the user keystore of a valid user via /data/data/com.tronlink.wallet/shared_prefs/<wallet-	N/A	A-TRO-WALL-130819/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			name>.xml to gain unauthorized access. **CVE ID : CVE-2019-13096**		
Information Exposure Through Log Files	22-07-2019	4	The user password via the registration form of TronLink Wallet 2.2.0 is stored in the log when the class CreateWalletTwoActivity is called. Other authenticated users can read it in the log later. The logged data can be read using Logcat on the device. When using platforms prior to Android 4.1 (Jelly Bean), the log data is not sandboxed per application; any application installed on the device has the capability to read data logged by other applications. **CVE ID : CVE-2019-13098**	N/A	A-TRO-WALL-130819/481
univention					
univention_corporate_server					
Information Exposure	17-07-2019	5	Univention Corporate Server univention-directory-notifier 12.0.1-3 and earlier is affected by: CWE-213: Intentional Information Exposure. The impact is: Loss of Confidentiality. The component is: function data_on_connection() in src/callback.c. The attack vector is: network connectivity. The fixed version is: 12.0.1-4 and later. **CVE ID : CVE-2019-1010283**	N/A	A-UNI-UNIV-130819/482
upwork					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
time_tracker					
N/A	23-07-2019	4.6	Upwork Time Tracker 5.2.2.716 doesn't verify the SHA256 hash of the downloaded program update before running it, which could lead to code execution or local privilege escalation by replacing the original update.exe. **CVE ID : CVE-2019-12162**	N/A	A-UPW-TIME-130819/483
vcftools_project					
vcftools					
Use After Free	25-07-2019	6.8	VCFTools vcftools prior to version 0.1.15 is affected by: Use-after-free. The impact is: Denial of Service or possibly other impact (eg. code execution or information disclosure). The component is: The header::add_FILTER_descriptor method in header.cpp. The attack vector is: The victim must open a specially crafted VCF file. **CVE ID : CVE-2019-1010127**	https://github.com/vcftools/vcftools/issues/141	A-VCF-VCFT-130819/484
Veeam					
one_reporter					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-07-2019	3.5	Veeam ONE Reporter 9.5.0.3201 allows XSS via the Add/Edit Widget with a crafted Caption field to setDashboardWidget in CommonDataHandlerReadOnly.ashx. **CVE ID : CVE-2019-14297**	N/A	A-VEE-ONE_-130819/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-07-2019	3.5	Veeam ONE Reporter 9.5.0.3201 allows XSS via a crafted Description(config) field to addDashboard or editDashboard in CommonDataHandlerReadOnly.ashx. **CVE ID : CVE-2019-14298**	N/A	A-VEE-ONE_-130819/486
Videolan					
vlc_media_player					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	4.3	libebml before 1.3.6, as used in the MKV module in VideoLAN VLC Media Player binaries before 3.0.3, has a heap-based buffer over-read in EbmlElement::FindNextElement. **CVE ID : CVE-2019-13615**	N/A	A-VID-VLC_-130819/487
Out-of-bounds Read	18-07-2019	7.5	lavc_CopyPicture in modules/codec/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height. **CVE ID : CVE-2019-13962**	N/A	A-VID-VLC_-130819/488
wcms					
wcms					
Cross-Site Request Forgery (CSRF)	23-07-2019	5.8	WCMS v0.3.2 has a CSRF vulnerability, with resultant directory traversal, to modify index.html via the /wex/html.php?finish=../index.html URI. **CVE ID : CVE-2019-14240**	N/A	A-WCM-WCMS-130819/489
webappick					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
woocommerce_product_feed					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-07-2019	4.3	WebAppick WooCommerce Product Feed 2.2.18 and earlier is affected by: Cross Site Scripting (XSS). The impact is: XSS to RCE via editing theme files in WordPress. The component is: admin/partials/woo-feed-manage-list.php:63. The attack vector is: Administrator must be logged in. **CVE ID : CVE-2019-1010124**	N/A	A-WEB-WOOC-130819/490
Wireshark					
wireshark					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	5	In Wireshark 3.0.0 to 3.0.2, 2.6.0 to 2.6.9, and 2.4.0 to 2.4.15, the ASN.1 BER dissector and related dissectors could crash. This was addressed in epan/asn1.c by properly restricting buffer increments. **CVE ID : CVE-2019-13619**	N/A	A-WIR-WIRE-130819/491
wp-code-highlightjs_project					
wp-code-highlightjs					
Cross-Site Request Forgery (CSRF)	19-07-2019	6.8	An issue was discovered in the wp-code-highlightjs plugin through 0.6.2 for WordPress. wp-admin/options-general.php?page=wp-code-highlight-js allows CSRF, as demonstrated by an XSS payload in the hljs_additional_css parameter. **CVE ID : CVE-2019-12934**	N/A	A-WP--WP-C-130819/492
wpeverest					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
everest_forms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-07-2019	7.5	A SQL injection vulnerability exists in WPEverest Everest Forms plugin for WordPress through 1.4.9. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via includes/evf-entry-functions.php **CVE ID : CVE-2019-13575**	N/A	A-WPE-EVER-130819/493
Zammad					
Zammad					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-07-2019	4.3	Zammad GmbH Zammad 2.3.0 and earlier is affected by: Cross Site Scripting (XSS) - CWE-80. The impact is: Execute java script code on users browser. The component is: web app. The attack vector is: the victim must open a ticket. The fixed version is: 2.3.1, 2.2.2 and 2.1.3. **CVE ID : CVE-2019-1010018**	N/A	A-ZAM-ZAMM-130819/494
zeek					
zeek					
NULL Pointer Dereference	17-07-2019	5	In Zeek Network Security Monitor (formerly known as Bro) before 2.6.2, a NULL pointer dereference in the Kerberos (aka KRB) protocol parser leads to DoS because a case-type index is mishandled. **CVE ID : CVE-2019-12175**	https://github.com/zeek/zeek/releases/tag/v2.6.2	A-ZEE-ZEEK-130819/495
Zohocorp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
manageengine_adselfservice_plus					
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. **CVE ID : CVE-2019-12876**	N/A	A-ZOH-MANA-130819/496
manageengine_admanager_plus					
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. **CVE ID : CVE-2019-12876**	N/A	A-ZOH-MANA-130819/497
manageengine_desktop_central					
N/A	17-07-2019	8.5	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System. **CVE ID : CVE-2019-12876**	N/A	A-ZOH-MANA-130819/498
zzcms					
zzmcms					
Improper Access Control	19-07-2019	7.5	zzcms zzmcms 8.3 and earlier is affected by: File Delete to getshell. The impact is: getshell. The component is: /user/ppsave.php. **CVE ID : CVE-2019-1010151**	N/A	A-ZZC-ZZMC-130819/499
zzcms					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	7.5	zzcms version 8.3 and earlier is affected by: SQL Injection. The impact is: zzcms File Delete to Code Execution. **CVE ID : CVE-2019-1010148**	N/A	A-ZZC-ZZCM-130819/500
Improper Input Validation	23-07-2019	7.5	zzcms version 8.3 and earlier is affected by: File Delete to Code Execution. The impact is: zzcms File Delete to Code Execution. The component is: user/licence_save.php. **CVE ID : CVE-2019-1010149**	N/A	A-ZZC-ZZCM-130819/501
Improper Input Validation	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: File Delete to Code Execution. The impact is: getshell. The component is: /user/zssave.php. **CVE ID : CVE-2019-1010150**	N/A	A-ZZC-ZZCM-130819/502
Improper Input Validation	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: File Delete to Code Execution. The impact is: getshell. The component is: user/manage.php line 31-80. **CVE ID : CVE-2019-1010152**	N/A	A-ZZC-ZZCM-130819/503
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-07-2019	7.5	zzcms 8.3 and earlier is affected by: SQL Injection. The impact is: sql inject. The component is: zs/subzs.php. **CVE ID : CVE-2019-1010153**	N/A	A-ZZC-ZZCM-130819/504

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
Operating System					
akuvox					
sp-r50p_firmware					
Use of Hard-coded Credentials	22-07-2019	10	Hardcoded credentials in the Akuvox R50P VoIP phone 50.0.6.156 allow an attacker to get access to the device via telnet. The telnet service is running on port 2323; it cannot be turned off and the credentials cannot be changed. **CVE ID : CVE-2019-12327**	N/A	O-AKU-SP-R-130819/505
Atcom					
a10w_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	22-07-2019	9	A command injection (missing input validation) issue in the remote phonebook configuration URI in the web interface of the Atcom A10W VoIP phone with firmware 2.6.1a2421 allows an authenticated remote attacker in the same network to trigger OS commands via shell metacharacters in a POST request. **CVE ID : CVE-2019-12328**	N/A	O-ATC-A10W-130819/506
Canonical					
ubuntu_linux					
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker	N/A	O-CAN-UBUN-130819/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2737**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Compiling). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N). **CVE ID : CVE-2019-2738**	N/A	O-CAN-UBUN-130819/508
Improper Access Control	23-07-2019	3.6	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent:	N/A	O-CAN-UBUN-130819/509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server: Security: Privileges). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2739**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable	N/A	O-CAN-UBUN-130819/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2740**		
Improper Access Control	23-07-2019	3.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2741**	N/A	O-CAN-UBUN-130819/511
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via	N/A	O-CAN-UBUN-130819/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L). **CVE ID : CVE-2019-2778**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/U	N/A	O-CAN-UBUN-130819/513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			I:N/S:U/C:L/I:L/A:N). **CVE ID : CVE-2019-2791**		
Improper Access Control	23-07-2019	2.3	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows high privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2797**	N/A	O-CAN-UBUN-130819/514
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability	N/A	O-CAN-UBUN-130819/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2757**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2758**	N/A	O-CAN-UBUN-130819/516
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported	N/A	O-CAN-UBUN-130819/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2774**		
Improper Access Control	23-07-2019	4	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI	N/A	O-CAN-UBUN-130819/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2019-2805**		
Improper Access Control	23-07-2019	5.5	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H). **CVE ID : CVE-2019-2819**	N/A	O-CAN-UBUN-130819/519
Improper Input Validation	17-07-2019	7.5	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9848	O-CAN-UBUN-130819/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executing arbitrary python commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9848**		
Information Exposure	17-07-2019	4	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9849**	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9849	O-CAN-UBUN-130819/521
chinamobileltd					
gpn2.4p21-c-cn_firmware					
Improper	19-07-2019	7.8	ChinaMobile GPN2.4P21-C-CN	N/A	O-CHI-GPN2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access Control			W2001EN-00 is affected by: Incorrect Access Control - Unauthenticated Remote Reboot. The impact is: PLC Wireless Router's are vulnerable to an unauthenticated remote reboot due. The component is: Reboot settings are available to unauthenticated users instead of only authenticaed users. The attack vector is: Remote. **CVE ID : CVE-2019-1010136**		130819/522
Cisco					
sg500-52mp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	N/A	O-CIS-SG50-130819/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1943		
sg500-52p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG50-130819/524
sg500x-24_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP	N/A	O-CIS-SG50-130819/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg500x-24p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG50-130819/526
sg500x-48_firmware					
URL Redirectio	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small	N/A	O-CIS-SG50-130819/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg500x-48p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL.	N/A	O-CIS-SG50-130819/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg500xg-8f8t_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG50-130819/529
spa500ds_firmware					
Improper Neutralization of Special Elements used in a	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The	N/A	O-CIS-SPA5-130819/530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('Command Injection')			vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
spa500s_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to	N/A	O-CIS-SPA5-130819/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
spa501g_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**	N/A	O-CIS-SPA5-130819/532
spa502g_firmware					
Improper	17-07-2019	4.6	A vulnerability in Cisco Small	N/A	O-CIS-SPA5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in a Command ('Command Injection')			Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		130819/533
spa504g_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a	N/A	O-CIS-SPA5-130819/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
spa508g_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5	N/A	O-CIS-SPA5-130819/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and prior. **CVE ID : CVE-2019-1923**		
spa509g_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**	N/A	O-CIS-SPA5-130819/536
spa512g_firmware					
Improper Neutralization of Special Elements used in a Command ('Comman	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in	N/A	O-CIS-SPA5-130819/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Injection')			the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
spa514g_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated	N/A	O-CIS-SPA5-130819/538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
aironet_3700e_firmware					
Improper Input Validation	17-07-2019	6.1	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly. **CVE ID : CVE-2019-1920**	N/A	O-CIS-AIRO-130819/539
aironet_3700i_firmware					
Improper Input Validation	17-07-2019	6.1	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The	N/A	O-CIS-AIRO-130819/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly. **CVE ID : CVE-2019-1920**		
aironet_3700p_firmware					
Improper Input Validation	17-07-2019	6.1	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly. **CVE ID : CVE-2019-1920**	N/A	O-CIS-AIRO-130819/541
spa525g2_firmware					
Improper Neutralization of Special	17-07-2019	4.6	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker	N/A	O-CIS-SPA5-130819/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior. **CVE ID : CVE-2019-1923**		
sf200-24_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user	N/A	O-CIS-SF20-130819/543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf200-24fp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF20-130819/544
sf200-24p_firmware					
URL Redirection to Untrusted Site ('Open	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated,	N/A	O-CIS-SF20-130819/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redirect')			remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf200-48_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing	N/A	O-CIS-SF20-130819/546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf200-48p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF20-130819/547
sf300-08_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of	N/A	O-CIS-SF30-130819/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf300-24_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf300-24mp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/550
sf300-24p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a	N/A	O-CIS-SF30-130819/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf300-24pp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/552
sf300-48_firmware					
URL Redirection to	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500	N/A	O-CIS-SF30-130819/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf300-48p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is	N/A	O-CIS-SF30-130819/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf300-48pp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/555
sf302-08_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page.	N/A	O-CIS-SF30-130819/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf302-08mp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious	N/A	O-CIS-SF30-130819/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sites. **CVE ID : CVE-2019-1943**		
sf302-08mpp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/558
sf302-08p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could	N/A	O-CIS-SF30-130819/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf302-08pp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF30-130819/560
sf500-24_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF50-130819/561
sf500-24p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web	N/A	O-CIS-SF50-130819/562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sf500-48_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SF50-130819/563
sf500-48p_firmware					
URL Redirection to Untrusted	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could	N/A	O-CIS-SF50-130819/564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Site ('Open Redirect')			allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-08_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect	N/A	O-CIS-SG20-130819/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-08p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG20-130819/566
sg200-10fp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to	N/A	O-CIS-SG20-130819/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-18_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	N/A	O-CIS-SG20-130819/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1943		
sg200-26_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG20-130819/569
sg200-26fp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP	N/A	O-CIS-SG20-130819/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-26p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG20-130819/571
sg200-50_firmware					
URL Redirectio	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small	N/A	O-CIS-SG20-130819/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n to Untrusted Site ('Open Redirect')			Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-50fp_firmware					
URL Redirectio n to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL.	N/A	O-CIS-SG20-130819/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg200-50p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG20-130819/574
sg300-10_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a	N/A	O-CIS-SG30-130819/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-10mp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to	N/A	O-CIS-SG30-130819/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-10mpp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/577
sg300-10p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP	N/A	O-CIS-SG30-130819/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-10pp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sg300-10sfp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/580
sg300-20_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a	N/A	O-CIS-SG30-130819/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-28_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/582
sg300-28mp_firmware					
URL Redirection to	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500	N/A	O-CIS-SG30-130819/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Site ('Open Redirect')			Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-28p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is	N/A	O-CIS-SG30-130819/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-28pp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/585
sg300-52_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page.	N/A	O-CIS-SG30-130819/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg300-52mp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious	N/A	O-CIS-SG30-130819/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sites. **CVE ID : CVE-2019-1943**		
sg300-52p_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG30-130819/588
sg500-28_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could	N/A	O-CIS-SG50-130819/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
sg500-28mpp_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG50-130819/590
sg500-28p_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**	N/A	O-CIS-SG50-130819/591
sg500-52_firmware					
URL Redirection to Untrusted Site ('Open Redirect')	17-07-2019	5.8	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web	N/A	O-CIS-SG50-130819/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites. **CVE ID : CVE-2019-1943**		
crossmatch					
digital_persona_u.are.u_4500_driver_firmware					
N/A	16-07-2019	4.3	An issue was discovered in the HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader Windows Biometric Framework driver 5.0.0.5. It has a statically coded initialization vector to encrypt a user's fingerprint image, resulting in weak encryption of that. This, in combination with retrieving an encrypted fingerprint image and encryption key (through another vulnerability), allows an attacker to obtain a user's fingerprint image. **CVE ID : CVE-2019-13603**	N/A	O-CRO-DIGI-130819/593
Debian					
debian_linux					
N/A	17-07-2019	7.2	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root	N/A	O-DEB-DEBI-130819/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments. **CVE ID : CVE-2019-13272**		
N/A	25-07-2019	10	Exim 4.85 through 4.92 (fixed in 4.92.1) allows remote code execution as root in some unusual configurations that use the ${sort } expansion for items that can be controlled by an attacker (e.g., $local_part or $domain). **CVE ID : CVE-2019-13917**	N/A	O-DEB-DEBI-130819/595
Dlink					
dsl-2750u_firmware					
Improper Authentication	23-07-2019	6.4	D-Link DSL-2750U 1.11 is affected by: Authentication Bypass. The impact is: denial of service and information leakage. The component is: login. **CVE ID : CVE-2019-1010155**	N/A	O-DLI-DSL--130819/596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fedoraproject					
fedora					
Improper Input Validation	16-07-2019	5	A vulnerability was discovered in DNS resolver of knot resolver before version 4.1.0 which allows remote attackers to downgrade DNSSEC-secure domains to DNSSEC-insecure state, opening possibility of domain hijack using attacks against insecure DNS protocol. **CVE ID : CVE-2019-10191**	https://www.knot-resolver.cz/2019-07-10-knot-resolver-4.1.0.html	O-FED-FEDO-130819/597
N/A	17-07-2019	7.2	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	N/A	O-FED-FEDO-130819/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13272		
Improper Input Validation	17-07-2019	7.5	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into executing arbitrary python commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9848**	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9848	O-FED-FEDO-130819/599
Information Exposure	17-07-2019	4	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed	https://www.libreoffice.org/about-us/security/advisories/CVE-2019-9849	O-FED-FEDO-130819/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5. **CVE ID : CVE-2019-9849**		
H3C					
h3cloud_os					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	19-07-2019	7.5	H3C H3Cloud OS all versions allows SQL injection via the ear/grid_event sidx parameter. **CVE ID : CVE-2019-12193**	N/A	O-H3C-H3CL-130819/601
htek					
uc902_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	9	The Htek UC902 VoIP phone web management interface contains several buffer overflow vulnerabilities in the firmware version 2.0.4.4.46, which allow an attacker to crash the device (DoS) without authentication or execute code (authenticated as a user) to spawn a remote shell as a root user. **CVE ID : CVE-2019-12325**	N/A	O-HTE-UC90-130819/602
Huawei					
honor_magic_2_firmware					
Information Exposure	17-07-2019	4.3	There is an information disclosure vulnerability on Secure Input of certain Huawei	N/A	O-HUA-HONO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			smartphones in Versions earlier than Tony-AL00B 9.1.0.216(C00E214R2P1). The Secure Input does not properly limit certain system privilege. An attacker tricks the user to install a malicious application and successful exploit could result in information disclosure. **CVE ID : CVE-2019-5222**		130819/603
linaro					
op-tee					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-07-2019	7.5	Linaro/OP-TEE OP-TEE Prior to version v3.4.0 is affected by: Boundary checks. The impact is: This could lead to corruption of any memory which the TA can access. The component is: optee_os. The fixed version is: v3.4.0. **CVE ID : CVE-2019-1010292**	N/A	O-LIN-OP-T-130819/604
Linksys					
re6400_firmware					
Improper Input Validation	17-07-2019	10	Unsanitized user input in the web interface for Linksys WiFi extender products (RE6400 and RE6300 through 1.2.04.022) allows for remote command execution. An attacker can access system OS configurations and commands that are not intended for use beyond the web UI. **CVE ID : CVE-2019-11535**	http://s3.amazonaws.com/downloads.linksys.com/support/assets/releasenotes/Linksys%20RE6300%20RE6400%20Firmware%20Release%20Notes_v1.2.05.001.tx	O-LIN-RE64-130819/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				t	
re6300_firmware					
Improper Input Validation	17-07-2019	10	Unsanitized user input in the web interface for Linksys WiFi extender products (RE6400 and RE6300 through 1.2.04.022) allows for remote command execution. An attacker can access system OS configurations and commands that are not intended for use beyond the web UI. **CVE ID : CVE-2019-11535**	http://s3.amazonaws.com/downloads.linksys.com/support/assets/releasenotes/Linksys%20RE6300%20RE6400%20Firmware%20Release%20Notes_v1.2.05.001.txt	O-LIN-RE63-130819/606
Linux					
linux_kernel					
Out-of-bounds Write	17-07-2019	4.6	In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages. **CVE ID : CVE-2019-13631**	N/A	O-LIN-LINU-130819/607
N/A	19-07-2019	4.9	In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects	N/A	O-LIN-LINU-130819/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arch/powerpc/kernel/signal_32.c and arch/powerpc/kernel/signal_64.c. **CVE ID : CVE-2019-13648**		
N/A	17-07-2019	7.2	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments. **CVE ID : CVE-2019-13272**	N/A	O-LIN-LINU-130819/609
Linuxfoundation					
open_network_operating_system					
Improper Input Validation	22-07-2019	7.5	The Linux Foundation ONOS 1.15.0 and ealier is affected by: Improper Input Validation. The impact is: The attacker	N/A	O-LIN-OPEN-130819/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can remotely execute any commands by sending malicious http request to the controller. The component is: Method runJavaCompiler in YangLiveCompilerManager.java. The attack vector is: network connectivity. **CVE ID : CVE-2019-1010234**		
Improper Input Validation	19-07-2019	7.5	The Linux Foundation ONOS SDN Controller 1.15 and earlier versions is affected by: Improper Input Validation. The impact is: A remote attacker can execute arbitrary commands on the controller. The component is: apps/yang/src/main/java/org/onosproject/yang/impl/YangLiveCompilerManager.java. The attack vector is: network connectivity. The fixed version is: 1.15. **CVE ID : CVE-2019-1010245**	N/A	O-LIN-OPEN-130819/611
Integer Overflow or Wraparound	18-07-2019	5.5	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Integer Overflow. The impact is: A network administrator (or attacker) can install unintended flow rules in the switch by mistake. The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The attack vector is: network management and connectivity. **CVE ID : CVE-2019-1010249**	N/A	O-LIN-OPEN-130819/612
Improper	18-07-2019	5.5	The Linux Foundation ONOS	N/A	O-LIN-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			2.0.0 and earlier is affected by: Poor Input-validation. The impact is: A network administrator (or attacker) can install unintended flow rules in the switch by mistake. The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The attack vector is: network management and connectivity. **CVE ID : CVE-2019-1010250**		130819/613
Improper Input Validation	18-07-2019	5.5	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Poor Input-validation. The impact is: A network administrator (or attacker) can install unintended flow rules in the switch by mistake. The component is: applyFlowRules() and apply() functions in FlowRuleManager.java. The attack vector is: network management and connectivity. **CVE ID : CVE-2019-1010252**	N/A	O-LIN-OPEN-130819/614
Paloaltonetworks					
pan-os					
Information Exposure	16-07-2019	6.5	Information disclosure in PAN-OS 7.1.23 and earlier, PAN-OS 8.0.18 and earlier, PAN-OS 8.1.8-h4 and earlier, and PAN-OS 9.0.2 and earlier may allow for an authenticated user with read-only privileges to extract the API key of the device and/or the	https://securityadvisories.paloaltonetworks.com/Home/Detail/157	O-PAL-PAN--130819/615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			username/password from the XML API (in PAN-OS) and possibly escalate privileges granted to them. **CVE ID : CVE-2019-1575**		
Improper Neutralization of Special Elements used in a Command ('Command Injection')	16-07-2019	6.5	Command injection in PAN-0S 9.0.2 and earlier may allow an authenticated attacker to gain access to a remote shell in PAN-OS, and potentially run with the escalated user?s permissions. **CVE ID : CVE-2019-1576**	https://securityadvisories.paloaltonetworks.com/Home/Detail/156	O-PAL-PAN--130819/616
Improper Input Validation	19-07-2019	6.8	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11-h1 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code. **CVE ID : CVE-2019-1579**	N/A	O-PAL-PAN--130819/617
Qualcomm					
qcs404_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/621
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
ipq8074_firmware					
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-IPQ8-130819/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-IPQ8-130819/624
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other	https://www.qualcom	O-QUA-IPQ8-130819/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	m.com/company/product-security/bulletins	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-IPQ8-130819/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ8-130819/627
qca6174a_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in	https://www.qualcomm.com/company/product-	O-QUA-QCA6-130819/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	security/bulletins	
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-QCA6-130819/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	bulletin	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/630
Out-of-bounds	25-07-2019	7.5	Out of bound access when reason code is extracted from	https://www.codeauro	O-QUA-QCA6-130819/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/633
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
qca6564_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA6-130819/635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
qca6574_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA6-130819/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
qca6574au_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA6-130819/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/638
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/640
Improper Restriction of Operations within the	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-QCA6-130819/641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	19/06/03/june-2019-code-aurora-security-bulletin	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/642

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2299**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/643
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA6-130819/645
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-QCA6-130819/646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	july-2019-code-aurora-security-bulletin	
qca6584_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA6-130819/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
qca6584au_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA6-130819/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
qca9377_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA9-130819/649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/650
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2305		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/653
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/655
qca9379_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-QCA9-130819/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	ulletins	
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-QCA9-130819/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	bulletin	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/658
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating	https://www.codeaurora.org/secu	O-QUA-QCA9-130819/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
qca9531_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA9-130819/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/664
qca9880_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in	https://www.qualcomm.com/company/product-	O-QUA-QCA9-130819/665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	security/bulletins	
qca9886_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA9-130819/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
qca9980_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA9-130819/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA9-130819/669
qcn5502_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCN5-130819/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
sd_665_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/672
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon	https://www.qualcomm.com/company/pro	O-QUA-SD_6-130819/673

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 MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	duct-security/bulletins	
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/675
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/677
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-	O-QUA-SD_6-130819/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/679
Improper Restriction of Operations	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified	https://www.qualcomm.com/company/pro	O-QUA-SD_6-130819/680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	duct-security/bulletins	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/681
Improper	25-07-2019	2.1	Out of bound read and	https://ww	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	w.qualcomm.com/company/product-security/bulletins	130819/682
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/684
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_6-130819/685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/687
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/689
qcs405_firmware					
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-QCS4-130819/690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	ulletins	
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/692
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2269		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/694
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/696
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/698
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/700
Improper Restriction of Operations within the Bounds of	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-QCS4-130819/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/702
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-130819/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/704
Improper Restriction of Operations within the	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity,	https://www.codeaurora.org/security-bulletin/20	O-QUA-QCS4-130819/705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	19/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/707
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS4-130819/708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
mdm9615_firmware					
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
mdm9625_firmware					
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/710
qca8081_firmware					
NULL Pointer Dereferenc	25-07-2019	2.1	Null pointer dereference during secure application termination using specific	https://www.qualcomm.com/co	O-QUA-QCA8-130819/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
e			application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	mpany/product-security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA8-130819/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA8-130819/713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCA8-130819/714
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCA8-130819/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
sd_730_firmware					
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/717
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/720
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://www.qualcomm.com/company/product-	O-QUA-SD_7-130819/721

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/723
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/726
Improper Restriction of Operations	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length	https://www.codeaurora.org/security-	O-QUA-SD_7-130819/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/728
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack	https://www.codeaurora.org/secu	O-QUA-SD_7-130819/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/730
Improper Restriction of Operations	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto,	https://www.codeaurora.org/security-	O-QUA-SD_7-130819/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/732
NULL Pointer	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip	https://www.qualcom	O-QUA-SD_7-130819/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	m.com/co mpany/pro duct-security/b ulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://ww w.qualcom m.com/co mpany/pro duct-security/b ulletins	O-QUA-SD_7-130819/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/735
Improper Restriction of Operations	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in	https://www.codeaurora.org/security-	O-QUA-SD_7-130819/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/737
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_7-130819/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/740
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/742
Improper Restriction	25-07-2019	4.6	When handling the vendor command there exists a	https://www.codeauro	O-QUA-SD_7-130819/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
mdm9635m_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
ipq4019_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-IPQ4-130819/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ4-130819/747
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ4-130819/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ4-130819/749
ipq8064_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in	https://www.qualcomm.com/company/product-	O-QUA-IPQ8-130819/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	security/bulletins	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-IPQ8-130819/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	bulletin	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ8-130819/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-IPQ8-130819/753
sd_600_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/756
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2307**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/759
mdm9206_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/761

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/762
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/764
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an	https://www.qualcomm.com/company/pro	O-QUA-MDM9-130819/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	duct-security/bulletins	
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/768
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/770

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
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/771
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-MDM9-130819/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/773
NULL Pointer Dereferenc	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in	https://www.qualcomm.com/co	O-QUA-MDM9-130819/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
e			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	mpany/product-security/bulletins	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/776
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/778
Out-of-bounds	25-07-2019	7.5	Out of bound access when reason code is extracted from	https://www.codeauro	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/779
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/780

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
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/781
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-MDM9-130819/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	aurora-security-bulletin	
mdm9607_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/784
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**		
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/786
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/790
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/793
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/796
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/ SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/798
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/799
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,	https://www.codeaurora.org/security-bulletin/20	O-QUA-MDM9-130819/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	19/06/03/june-2019-code-aurora-security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/802
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-MDM9-130819/803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/804
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-MDM9-130819/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/807
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/809
Out-of-	25-07-2019	7.5	While storing calibrated data	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	MDM9-130819/810
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
mdm9650_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/812
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/b	O-QUA-MDM9-130819/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	ulletins	
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2237**		
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/815
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/818
Improper Restriction	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while	https://www.qualcom	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	m.com/company/product-security/bulletins	130819/819
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/821
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free	https://www.codeaurora.org/secu	O-QUA-MDM9-130819/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	rity-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/824
Improper Restriction of Operations	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length	https://www.codeaurora.org/security-	O-QUA-MDM9-130819/825

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/826
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,	https://www.codeaurora.org/security-bulletin/20	O-QUA-MDM9-130819/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	19/06/03/june-2019-code-aurora-security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/829
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-MDM9-130819/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/831
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2299		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/834
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/836
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message	https://www.codeaurora.org/security-	O-QUA-MDM9-130819/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2309**		
mdm9655_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/839
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/842
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/845
msm8996au_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/849
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://www.qualcomm.com/company/product-	O-QUA-MSM8-130819/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/852
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/855
Improper Restriction of Operations within the	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto,	https://www.codeaurora.org/security-bulletin/20	O-QUA-MSM8-130819/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	19/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/857
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto,	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-MSM8-130819/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/859
Improper Restriction of Operations within the Bounds of a Memory	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-	O-QUA-MSM8-130819/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	code-aurora-security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/862
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-MSM8-130819/863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	bulletin	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/864
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-MSM8-130819/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/866
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-MSM8-130819/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/868
Out-of-	25-07-2019	7.5	Out of bound access when	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	MSM8-130819/869
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/871
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-MSM8-130819/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/873
Improper	25-07-2019	4.6	When handling the vendor	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	MSM8-130819/874
sd_410_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2236		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/877
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2238		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/879
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_4-130819/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	ulletins	
sd_412_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/883
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/885
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/886

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 Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
sd_820a_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/888
Improper Input	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI	https://www.qualcom	O-QUA-SD_8-130819/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	m.com/company/product-security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/892
Improper Input	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a	https://www.qualcom	O-QUA-SD_8-130819/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	m.com/company/product-security/bulletins	
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/895
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other	https://www.qualcom	O-QUA-SD_8-130819/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	m.com/company/product-security/bulletins	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/898
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/900
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/902
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/904
Improper Restriction of	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient	https://www.qualcomm.com/co	O-QUA-SD_8-130819/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	mpany/product-security/bulletins	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/906
Out-of-	22-07-2019	7.5	Improper validation for inputs	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	w.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	130819/907
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 /	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/909
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/911
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_8-130819/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/913
Improper Restriction of	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display	https://www.codeaurora.org/secu	O-QUA-SD_8-130819/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/916
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_8-130819/917

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/918
qualcomm_215_firmware					
Improper Restriction	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to	https://www.qualcom	O-QUA-QUAL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	m.com/company/product-security/bulletins	130819/919
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/922
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information 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	O-QUA-QUAL-130819/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/925
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-QUAL-130819/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/928
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-130819/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/931
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QUAL-130819/933
sd_205_firmware					
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**		
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/935
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/939
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/942
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/945
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/947
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/949
Improper Restriction of Operations within the	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from	https://www.qualcomm.com/company/product-	O-QUA-SD_2-130819/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	security/bulletins	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/952
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/954
Improper Restriction of Operations	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto,	https://www.codeaurora.org/security-	O-QUA-SD_2-130819/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/957
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
sd_210_firmware					
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/959
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_2-130819/960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	ulletins	
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/963
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/965
Informatio	25-07-2019	7.5	Position determination	https://ww	O-QUA-SD_2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	w.qualcomm.com/company/product-security/bulletins	130819/966
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/969
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/971
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/973
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/976
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SD_2-130819/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/978
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_2-130819/979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/981
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SD_2-130819/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/983
sd_212_firmware					
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation	https://www.qualcomm.com/co	O-QUA-SD_2-130819/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	mpany/product-security/bulletins	
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/985
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to	https://www.qualcomm.com/co	O-QUA-SD_2-130819/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	mpany/product-security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/989
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in	https://www.qualcomm.com/co	O-QUA-SD_2-130819/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	mpany/product-security/bulletins	
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/992
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory	https://www.qualcomm.com/co	O-QUA-SD_2-130819/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	mpany/product-security/bulletins	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/995
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/997
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SD_2-130819/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-130819/1000
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1002
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SD_2-130819/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	security/bulletins	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1005
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_2-130819/1007
Improper Restriction of Operations	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of	https://www.codeaurora.org/security-	O-QUA-SD_2-130819/1008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
sd_415_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1010
Improper	25-07-2019	7.5	Buffer over-read can occur	https://ww	O-QUA-SD_4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	w.qualcomm.com/company/product-security/bulletins	130819/1011
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1013
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
sd_425_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1016
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1017

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 IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1020
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1023
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1024

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 IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1026
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1028
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**		
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1030
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2279		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1032
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1034
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1036
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto,	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_4-130819/1037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	19/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1038
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon	https://www.codeaurora.org/security-	O-QUA-SD_4-130819/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1040
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-SD_4-130819/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1043
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1045
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_4-130819/1046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1048
sd_427_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1051
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD_4-130819/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	security/bulletins	
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1053

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1054
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-SD_4-130819/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	june-2019-code-aurora-security-bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1056

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1057
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-	O-QUA-SD_4-130819/1058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1059
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1061
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 /	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_4-130819/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1063
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1065
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1067
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access	https://www.codeaurora.org/secu	O-QUA-SD_4-130819/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1069
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to	https://www.codeauro	O-QUA-SD_4-130819/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1071
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_4-130819/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	19/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1074
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_4-130819/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	security-bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2308		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1077
sd_429_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1079

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1080
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD_4-130819/1081

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	security/bulletins	
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1083
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-SD_4-130819/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	june-2019-code-aurora-security-bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1086
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1088
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1091
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SD_4-130819/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1093
sd_430_firmware					
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_4-130819/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	ulletins	
NULL Pointer Dereferenc e	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD	https://ww w.qualcom m.com/co mpany/pro duct-security/b ulletins	O-QUA-SD_4-130819/1095

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
			427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1097
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1100
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure 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	O-QUA-SD_4-130819/1101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1103
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1105
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2277		
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1107
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1109
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1111
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1113
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1115
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1117
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_4-130819/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1120
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1122
sd_435_firmware					
Improper Restriction of	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the	https://www.qualcomm.com/co	O-QUA-SD_4-130819/1123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	mpany/product-security/bulletins	
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1126
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1129
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1132
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2272		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1134
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24 **CVE ID : CVE-2019-2277**		
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1136
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1138
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1140
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1142
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-	O-QUA-SD_4-130819/1143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1144
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1146
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_4-130819/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	19/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1149
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1151
sd_439_firmware					
Improper Restriction	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to	https://www.qualcom	O-QUA-SD_4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	m.com/company/product-security/bulletins	130819/1152
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1155
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1158
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1160
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://www.qualcomm.com/co	O-QUA-SD_4-130819/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	mpany/product-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1163
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1166
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
sd_450_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1168
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_4-130819/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	ulletins	
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1172
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1175
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1177
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SD_4-130819/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	bulletin	
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1179
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-	O-QUA-SD_4-130819/1180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	aurora-security-bulletin	
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1181
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1183
Improper Restriction of Operations within the Bounds of	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_4-130819/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	ulletins	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1185
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper	https://www.qualcomm.com/company/pro	O-QUA-SD_4-130819/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	duct-security/bulletins	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1188
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1190
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-130819/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1192
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1193

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1194
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_4-130819/1195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1197
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_4-130819/1198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
sd_615_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1200
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1203
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1205
sd_616_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_6-130819/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1208
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded	https://www.qualcomm.com/co	O-QUA-SD_6-130819/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	mpany/product-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1211
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_6-130819/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	aurora-security-bulletin	
sd_625_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1214
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_6-130819/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1218
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1221
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto,	https://www.codeaurora.org/security-	O-QUA-SD_6-130819/1222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1223
Improper Restriction	22-07-2019	7.5	Possible buffer overflow while processing the high level lim	https://www.codeauro	O-QUA-SD_6-130819/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	ra.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1225
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://www.qualcomm.com/co	O-QUA-SD_6-130819/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	mpany/product-security/bulletins	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1227
Improper Authentica	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to	https://www.codeauro	O-QUA-SD_6-130819/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion			bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1229
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_6-130819/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1232
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1234
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1236
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1238
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1240
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-SD_6-130819/1241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1243
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1245
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_6-130819/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	july-2019-code-aurora-security-bulletin	
sd_632_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1248
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in	https://www.qualcomm.com/company/pro	O-QUA-SD_6-130819/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	duct-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1251
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due	https://www.qualcom	O-QUA-SD_6-130819/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	m.com/company/product-security/bulletins	
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2261**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1255
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1257
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1260
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1262
sd_636_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1265

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1266
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://www.qualcomm.com/company/product-	O-QUA-SD_6-130819/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1269
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1272
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto,	https://www.codeaurora.org/security-	O-QUA-SD_6-130819/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1274
Improper Restriction	22-07-2019	7.5	Possible buffer overflow while processing the high level lim	https://www.codeauro	O-QUA-SD_6-130819/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	ra.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1276
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack	https://www.codeaurora.org/secu	O-QUA-SD_6-130819/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1278
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon	https://www.codeaurora.org/security-	O-QUA-SD_6-130819/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1280
Improper Restriction of Operations within the Bounds of a Memory	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1282
Improper Restriction of Operations	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded	https://www.qualcomm.com/company/pro	O-QUA-SD_6-130819/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	duct-security/bulletins	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1284
Improper Validation	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when	https://www.qualcom	O-QUA-SD_6-130819/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Array Index			scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	m.com/company/product-security/bulletins	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1287
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1289
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2298		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1291
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1293
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_6-130819/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1296
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1298
sd_650_firmware					
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_6-130819/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	ulletins	
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1301

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1302
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_6-130819/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1304
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://www.qualcomm.com/co	O-QUA-SD_6-130819/1305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	mpany/product-security/bulletins	
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd_652_firmware					
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1307
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2261		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1311
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1313
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
sda660_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1315
NULL Pointer	25-07-2019	2.1	Null pointer dereference during secure application	https://www.qualcom	O-QUA-SDA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereferenc e			termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	m.com/co mpany/pro duct-security/b ulletins	130819/1316
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://ww w.qualcom m.com/co mpany/pro duct-security/b ulletins	O-QUA-SDA6-130819/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1320
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1323
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SDA6-130819/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1325
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1327
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1330
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDA6-130819/1331
Out-of-	22-07-2019	7.5	Improper validation for inputs	https://ww	O-QUA-SDA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	w.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	130819/1332
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1334
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDA6-130819/1336
sdm439_firmware					
Improper Restriction	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to	https://www.qualcom	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	m.com/company/product-security/bulletins	130819/1337
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1340
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1343
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1345
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in	https://www.qualcomm.com/co	O-QUA-SDM4-130819/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	mpany/product-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1348
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-130819/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1351
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM4-130819/1353
sdm630_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1355

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
			675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1357
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading	https://www.qualcomm.com/company/product-	O-QUA-SDM6-130819/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1360
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1363
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-	O-QUA-SDM6-130819/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1365
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SDM6-130819/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	aurora-security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1367
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SDM6-130819/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1369
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1372
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1374
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SDM6-130819/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1376
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SDM6-130819/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1379
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
sdm660_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1382
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1386
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1388

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
			SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1389
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure 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	O-QUA-SDM6-130819/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1392
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1393
Improper	25-07-2019	4.6	Buffer overflow can occur in	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/1394
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1395
Out-of-	22-07-2019	4.6	Out of bound read can happen	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	w.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	130819/1396
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1397
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-	O-QUA-SDM6-130819/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1399
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1402
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1404
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1406
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24 **CVE ID : CVE-2019-2293**		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-130819/1408
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1410
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SDM6-130819/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1412
Integer	25-07-2019	10	Possible integer underflow	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/1413
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDM6-130819/1415
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SDM6-130819/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	bulletin	
snapdragon_high_med_2016_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1418
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SNAP-130819/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1422
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SNAP-130819/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1424
Improper Restriction of Operations within the	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity,	https://www.codeaurora.org/security-bulletin/20	O-QUA-SNAP-130819/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	19/06/03/june-2019-code-aurora-security-bulletin	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-130819/1427
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SNAP-130819/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	aurora-security-bulletin	
mdm9150_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1431
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1434
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1436
Improper Restriction	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead	https://www.codeauro	O-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	ra.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	130819/1437
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1439
Improper Restriction of Operations within the Bounds of	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-MDM9-130819/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1441
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-MDM9-130819/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	19/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1444
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-MDM9-130819/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	security-bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2308		
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1447
mdm9640_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1451
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1453
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-MDM9-130819/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SDM660 **CVE ID : CVE-2019-2278**	bulletin	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1455
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-130819/1457
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-MDM9-130819/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1460
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MDM9-130819/1462
msm8909w_firmware					
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-130819/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	security/bulletins	
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/1464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/1465
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-MSM8-130819/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1467

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1468
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2272		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/1470
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/1472
Improper Restriction of Operations within the Bounds of	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-MSM8-130819/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	ulletins	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1474
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in	https://www.codeaurora.org/security-	O-QUA-MSM8-130819/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1477
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-130819/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1479
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-MSM8-130819/1481
qcs605_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1484
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1486
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly	https://www.qualcomm.com/co	O-QUA-QCS6-130819/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	mpany/product-security/bulletins	
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1488

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 Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1490
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1493
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-	O-QUA-QCS6-130819/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1495
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1497
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-QCS6-130819/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1499
Improper Restriction of Operations within the	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-QCS6-130819/1500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	security/bulletins	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1501
Improper Restriction	25-07-2019	2.1	Out of bound read and information disclosure in	https://www.qualcom	O-QUA-QCS6-130819/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	m.com/company/product-security/bulletins	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1504
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1505

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1506
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1508
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-130819/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1510
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-QCS6-130819/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1512
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-QCS6-130819/1513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1515
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-QCS6-130819/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
sd_670_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2235		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1518
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**		
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1520
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1524
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1527
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1530
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1532
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1534
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2277		
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1536
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1537
Improper Restriction	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to	https://www.qualcom	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	m.com/company/product-security/bulletins	130819/1538
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2334		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1540
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1542
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1544
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-	O-QUA-SD_6-130819/1545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1546
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1548
Improper Restriction of Operations within the	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_6-130819/1549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	19/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1550
Improper Restriction	25-07-2019	4.6	Improper casting of structure while handling the buffer leads	https://www.codeauro	O-QUA-SD_6-130819/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1553
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_6-130819/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1555
sd_675_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1556
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**		
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1558
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1562
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1565
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1567
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-	O-QUA-SD_6-130819/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1569
Improper Restriction of	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently	https://www.qualcomm.com/co	O-QUA-SD_6-130819/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	mpany/product-security/bulletins	
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-130819/1572
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1574
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1577
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_6-130819/1579
Improper Restriction of Operations within the Bounds of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_6-130819/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Memory Buffer			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	july-2019-code-aurora-security-bulletin	
sd_710_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1582
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure	https://www.qualcomm.com/company/pro	O-QUA-SD_7-130819/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	duct-security/bulletins	
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1584
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in	https://www.qualcomm.com/company/pro	O-QUA-SD_7-130819/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	duct-security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1588
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/pro	O-QUA-SD_7-130819/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	duct-security/bulletins	
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1590

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1591
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information	https://www.qualcomm.com/company/pro	O-QUA-SD_7-130819/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	duct-security/bulletins	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1594
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1596
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1598
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**		
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1600
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1602
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1604
Concurrent Execution using Shared Resource with Improper	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-SD_7-130819/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	code-aurora-security-bulletin	
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1606
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1608
Improper Restriction of Operations within the	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_7-130819/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	19/06/03/june-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1610
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**		
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1613
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1615
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1617
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur	https://www.codeaurora.org/secu	O-QUA-SD_7-130819/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**		
sd_712_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1620
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1623
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1626
Improper Restriction of Operations within the	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SD_7-130819/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	security/bulletins	
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1629
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/06/03/	O-QUA-SD_7-130819/1630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	june-2019-code-aurora-security-bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1631

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1632
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-	O-QUA-SD_7-130819/1633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1634
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1636
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_7-130819/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1638
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-	O-QUA-SD_7-130819/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SDM660 **CVE ID : CVE-2019-2278**	bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1640
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1642
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1644
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1646
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead	https://www.codeauro	O-QUA-SD_7-130819/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1648
Use After	25-07-2019	4.6	Pointer dereference while	https://ww	O-QUA-SD_7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/1649
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-130819/1650
Integer Overflow or Wraparou	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in	https://www.codeaurora.org/security-	O-QUA-SD_7-130819/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nd			Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1653
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1655
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the	https://www.codeaurora.org/secu	O-QUA-SD_7-130819/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_7-130819/1658
sd_820_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1661
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an	https://www.qualcomm.com/company/pro	O-QUA-SD_8-130819/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**	duct-security/bulletins	
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1665
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1668
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SD_8-130819/1669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	security-bulletin	
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1670
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-	O-QUA-SD_8-130819/1671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1672
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/b	O-QUA-SD_8-130819/1673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	ulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1675
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1676

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2346		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1677
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**		
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1679
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2305		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1682
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1684
sd_835_firmware					
Improper Restriction of	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the	https://www.qualcomm.com/co	O-QUA-SD_8-130819/1685

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**	mpany/product-security/bulletins	
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1686

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2240		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1689
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1691
Informatio	25-07-2019	7.5	Position determination	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n Exposure			accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	w.qualcomm.com/company/product-security/bulletins	130819/1692
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1695
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1697
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX24 **CVE ID : CVE-2019-2277**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1699
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1701
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1703
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1705
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead	https://www.codeauro	O-QUA-SD_8-130819/1706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1707
Integer	25-07-2019	4.6	An out-of-bound write can be	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/1708
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1710
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_8-130819/1711

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 in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	19/07/01/july-2019-code-aurora-security-bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1712

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1713
sd_845_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1717
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1720
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-	O-QUA-SD_8-130819/1721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	aurora-security-bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1723
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SD_8-130819/1724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1725
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1727
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1729
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2278		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1731
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**		
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1733
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1735
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1737
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access	https://www.codeaurora.org/secu	O-QUA-SD_8-130819/1738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1739
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to	https://www.codeauro	O-QUA-SD_8-130819/1740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1741
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon	https://www.codeaurora.org/security-bulletin/20	O-QUA-SD_8-130819/1742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	19/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1744
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1746
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the	https://www.codeaurora.org/secu	O-QUA-SD_8-130819/1747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-2309**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1749
sd_850_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1753
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. 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	O-QUA-SD_8-130819/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1756
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-	O-QUA-SD_8-130819/1757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	bulletin	
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1759
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1761
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**		
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1763
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1765
Improper Authentication	25-07-2019	7.2	User keystore signature is ignored in boot and can lead to bypass boot image signature verification in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in MDM9607, MDM9640, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 845 / SD 850, SDM660 **CVE ID : CVE-2019-2278**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1766
Improper Restriction	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead	https://www.codeauro	O-QUA-SD_8-130819/1767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	ra.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1769
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1771
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**		
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1773
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-SD_8-130819/1774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1775
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/	O-QUA-SD_8-130819/1776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	july-2019-code-aurora-security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1777
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-	O-QUA-SD_8-130819/1778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1779
Out-of-bounds	25-07-2019	7.5	Out of bound access when reason code is extracted from	https://www.codeauro	O-QUA-SD_8-130819/1780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**		
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1782
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SD_8-130819/1783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	While storing calibrated data from firmware in cache, An integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1784
Improper Restriction	25-07-2019	4.6	When handling the vendor command there exists a	https://www.codeauro	O-QUA-SD_8-130819/1785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
sd_855_firmware					
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 /	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	2.1	Possible buffer overflow at the end of iterating loop while getting the version info and lead to information disclosure. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660 **CVE ID : CVE-2019-2243**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1788
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1791
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1793
Out-of-	25-07-2019	7.8	IOMMU page fault while	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	w.qualcomm.com/company/product-security/bulletins	130819/1794
Out-of-bounds Read	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2276		
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1796
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1798
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1800
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon	https://www.qualcomm.com/company/product-	O-QUA-SD_8-130819/1801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	security/bulletins	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2287		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1803
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1804
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-	https://www.qualcomm.com/co	O-QUA-SD_8-130819/1805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	mpany/product-security/bulletins	
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 /	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1806

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1807
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1809
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-	O-QUA-SD_8-130819/1810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**	code-aurora-security-bulletin	
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SD_8-130819/1812
sdx20_firmware					
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**		
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	7.5	Buffer over-read can occur while parsing an ogg file with a corrupted comment block. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2253**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1815

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1816
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-	O-QUA-SDX2-130819/1817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	bulletin	
Use After Free	25-07-2019	4.6	Access to freed memory can happen while reading from diag driver due to use after free issue in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA9531, QCA9980, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2263**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1819
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow can occur in display function due to lack of validation of header block size set by user. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2272**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1820
Improper	22-07-2019	7.5	Shared memory gets updated	https://ww	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	w.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	130819/1821
NULL Pointer Dereference	25-07-2019	7.8	Null pointer dereferencing can happen when playing the clip with wrong block group id in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2334**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1823
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**		
Use After Free	25-07-2019	4.6	Multiple open and close from multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1825
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150,	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-	O-QUA-SDX2-130819/1826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	security-bulletin	
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1827
Integer Overflow or Wraparound	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-	O-QUA-SDX2-130819/1828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	aurora-security-bulletin	
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Improper casting of structure while handling the buffer leads to out of bound read in display in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-2306**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1830
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1832
Out-of-bounds	25-07-2019	7.5	While storing calibrated data from firmware in cache, An	https://www.codeauro	O-QUA-SDX2-130819/1833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			integer overflow may occur since data length received may exceed real data length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 845 / SD 850, SDM660, SDX20 **CVE ID : CVE-2019-2309**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
sxr1130_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1835
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case	https://www.qualcom	O-QUA-SXR1-130819/1836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	m.com/company/product-security/bulletins	
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1837
Improper Input	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI	https://www.qualcom	O-QUA-SXR1-130819/1838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	m.com/company/product-security/bulletins	
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1839

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1840

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2019-2254**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2260**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SXR1-130819/1842
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure 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	O-QUA-SXR1-130819/1843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SXR1-130819/1844
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/pro	O-QUA-SXR1-130819/1845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**	duct-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-130819/1846
Improper Restriction of Operations within the	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from	https://www.qualcomm.com/company/product-	O-QUA-SXR1-130819/1847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**	security/bulletins	
sd_8cx_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Buffer overflow occurs when emulated RPMB is used due to sector size assumptions in the TA rollback protection logic. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2235**		
NULL Pointer Dereference	25-07-2019	2.1	Null pointer dereference during secure application termination using specific application ids. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2236**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	25-07-2019	2.1	Failure in taking appropriate action to handle the error case If keypad gpio deactivation fails leads to silent failure scenario and subsequent logic gets executed everytime in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2237**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1850
Out-of-bounds Read	25-07-2019	4.6	Lack of check of data type can lead to subsequent loop-expression potentially go negative and the condition will still evaluate to true leading to buffer underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9206, MDM9607, MDM9650, MDM9655, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 8CX, SXR1130 **CVE ID : CVE-2019-2238**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1852
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1853

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour 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	O-QUA-SD_8-130819/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Information Exposure	25-07-2019	7.5	Position determination accuracy may be degraded due to wrongly decoded information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1855

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2254**		
N/A	22-07-2019	4.9	Unauthorized access from GPU subsystem to HLOS or other non secure subsystem memory can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9150, MDM9206, MDM9607, MDM9650, MSM8996AU, QCA8081, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2261**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1856
Out-of-bounds Read	25-07-2019	7.8	IOMMU page fault while playing h265 video file leads to denial of service issue in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 650/52, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 845 / SD 850, SD 855, SD 8CX, SDM439, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2273**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1858
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	2.1	Out of bound read and information disclosure in firmware due to insufficient checking of an embedded structure that can be sent from a kernel driver in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1859

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2343**		
Improper Validation of Array Index	25-07-2019	7.2	Firmware is getting into loop of overwriting memory when scan command is given from host because of improper validation. in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ8074, QCA8081, QCS404, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660 **CVE ID : CVE-2019-2346**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-130819/1860
sdx24_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	25-07-2019	2.1	Sanity checks are missing in layout which can lead to SUI Corruption or can lead to Denial of Service in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9206, MDM9607, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2239**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1861
N/A	25-07-2019	2.1	While sending the rendered surface content to the screen, Error handling is not properly checked results in an unpredictable behaviour in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1862

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6564, QCA6574, QCA6574AU, QCA6584, QCA6584AU, QCA8081, QCA9377, QCA9379, QCA9531, QCA9880, QCA9886, QCA9980, QCN5502, QCS404, QCS605, SD 210/SD 212/SD 205, SD 425, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2240**		
Improper Input Validation	25-07-2019	2.1	While rendering the layout background, Error status check is not caught properly and also incorrect status handling is being done leading to unintended SUI behaviour 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	O-QUA-SDX2-130819/1863

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, QCS404, QCS605, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2241**		
Use After Free	22-07-2019	6.9	A race condition occurs while processing perf-event which can lead to a use after free condition in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016, SXR1130	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1864

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2260		
NULL Pointer Dereference	22-07-2019	4.6	Null pointer dereference occurs for channel context while opening glink channel in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9607, MDM9640, MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670, SD 820A, SD 835, SD 845 / SD 850, SDM439, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2264**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1865
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	7.5	Possible buffer overflow while processing the high level lim process action frame due to improper buffer length validation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCS405, QCS605, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-2269**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1866
Out-of-bounds	25-07-2019	10	Possible out of bound read occurs while processing beaconing request due to lack	https://www.codeaurora.org/secu	O-QUA-SDX2-130819/1867

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			of check on action frames received from user controlled space in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2276**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Read	22-07-2019	4.6	Out of bound read can happen due to lack of NULL termination on user controlled data in WLAN in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MSM8996AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2277**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1868
Improper Restriction of Operations	22-07-2019	7.5	Shared memory gets updated with invalid data and may lead to access beyond the allocated memory. in Snapdragon Auto,	https://www.codeaurora.org/security-	O-QUA-SDX2-130819/1869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2279**	bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	An unauthenticated bitmap image can be loaded in to memory and subsequently cause execution of unverified code. in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS405, QCS605, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX24, SXR1130 **CVE ID : CVE-2019-2281**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1870
Concurrent Execution	25-07-2019	4.4	Race condition while accessing DMA buffer in jpeg driver in	https://www.codeauro	O-QUA-SDX2-130819/1871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2345**	ra.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Out-of-bounds Write	22-07-2019	7.5	Improper validation for inputs received from firmware can lead to an out of bound write issue in video driver. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2287**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1872
Use After	25-07-2019	4.6	Multiple open and close from	https://ww	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			multiple threads will lead camera driver to access destroyed session data pointer in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDM660, SDX20, SDX24, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-2290**	w.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	130819/1873
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-07-2019	4.6	Out of bound access can occur due to buffer copy without checking size of input received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9650, MSM8996AU, QCA6574AU, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2292**	https://www.codeaurora.org/security-bulletin/2019/06/03/june-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1874

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	25-07-2019	4.6	Pointer dereference while freeing IFE resources due to lack of length check of in port resource. in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2293**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1875
Use After Free	25-07-2019	4.6	Protection is missing while accessing md sessions info via macro which can lead to use-after-free in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2298**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDX2-130819/1876
Integer Overflow or	25-07-2019	4.6	An out-of-bound write can be triggered by a specially-crafted command supplied by a	https://www.codeaurora.org/secu	O-QUA-SDX2-130819/1877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			userspace application. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2299**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-07-2019	4.6	Possibility of out-of-bound read if id received from SPI is not in range of FIFO in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9980, QCS605, Qualcomm 215, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 712 / SD 710 / SD 670,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SD 820A, SD 845 / SD 850, SD 855, SDM439, SDM660, SDX24 **CVE ID : CVE-2019-2301**		
Out-of-bounds Read	25-07-2019	7.5	Out of bound access when reason code is extracted from frame data without validating the frame length in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2305**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1879
Integer Underflow (Wrap or Wraparound)	25-07-2019	10	Possible integer underflow due to lack of validation before calculation of data length in 802.11 Rx management configuration in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9640,	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2307**		
N/A	25-07-2019	7.2	User application could potentially make RPC call to the fastrpc driver and the driver will allow the message to go through to the remote subsystem in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2308**	https://www.codeaurora.org/security-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	O-QUA-SDX2-130819/1881
Improper Restriction of	25-07-2019	4.6	When handling the vendor command there exists a potential buffer overflow due	https://www.codeaurora.org/secu	O-QUA-SDX2-130819/1882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			to lack of input validation of data buffer received in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9607, MDM9640, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, QCS605, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDM630, SDM660, SDX24 **CVE ID : CVE-2019-2312**	rity-bulletin/2019/07/01/july-2019-code-aurora-security-bulletin	
Tp-link					
archer_c1200_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-07-2019	7.5	CMD_SET_CONFIG_COUNTRY in the TP-Link Device Debug protocol in TP-Link Archer C1200 1.0.0 Build 20180502 rel.45702 and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server. **CVE ID : CVE-2019-13614**	N/A	O-TP--ARCH-130819/1883
Zeroshell					
zeroshell					
Improper Neutralizat	19-07-2019	10	Zeroshell 3.9.0 is prone to a remote command execution	N/A	O-ZER-ZERO-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion of Special Elements used in an OS Command ('OS Command Injection')			vulnerability. Specifically, this issue occurs because the web application mishandles a few HTTP parameters. An unauthenticated attacker can exploit this issue by injecting OS commands inside the vulnerable parameters. **CVE ID : CVE-2019-12725**		130819/1884
ZTE					
otcp_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-07-2019	2.3	All versions up to V1.19.20.02 of ZTE OTCP product are impacted by XSS vulnerability. Due to XSS, when an attacker invokes the security management to obtain the resources of the specified operation code owned by a user, the malicious script code could be transmitted in the parameter. If the front end does not process the returned result from the interface properly, the malicious script may be executed and the user cookie or other important information may be stolen. **CVE ID : CVE-2019-3414**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1010883	O-ZTE-OTCP-130819/1885