National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Nov 2019 Vol. 06 No. 21

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
admincolumns					
admin_columns					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	08-11-2019	9	A CSV injection in the codepress-admin-columns (aka Admin Columns) plugin 3.4.6 for WordPress allows malicious users to gain remote control of other computers. By choosing formula code as his first or last name, an attacker can create a user with a name that contains malicious code. Other users might download this data as a CSV file and corrupt their PC by opening it in a tool such as Microsoft Excel. The attacker could gain remote access to the user's PC. **CVE ID : CVE-2019-17661**	N/A	A-ADM-ADMI-271119/1
Apache					
impala					
Missing Authentication for Critical Function	05-11-2019	4.6	In Apache Impala 2.7.0 to 3.2.0, an authenticated user with access to the IDs of active Impala queries or sessions can interact with those sessions or queries via a specially-constructed request and thereby potentially bypass authorization and audit	https://lists.apache.org/thread.html/ee73dd8dc38ac3b3b132c79c9a02cf9524af9aa11190474c0ebd1f13@%3Cdev.i	A-APA-IMPA-271119/2

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mechanisms. Session and query IDs are unique and random, but have not been documented or consistently treated as sensitive secrets. Therefore they may be exposed in logs or interfaces. They were also not generated with a cryptographically secure random number generator, so are vulnerable to random number generator attacks that predict future IDs based on past IDs. Impala deployments with Apache Sentry or Apache Ranger authorization enabled may be vulnerable to privilege escalation if an authenticated attacker is able to hijack a session or query from another authenticated user with privileges not assigned to the attacker. Impala deployments with audit logging enabled may be vulnerable to incorrect audit logging as a user could undertake actions that were logged under the name of a different authenticated user. Constructing an attack requires a high degree of technical sophistication and access to the Impala system as an authenticated user. **CVE ID : CVE-2019-10084**	mpala.apache.org%3E	
cxf					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	06-11-2019	4.3	Apache CXF before 3.3.4 and 3.2.11 does not restrict the number of message attachments present in a given message. This leaves open the possibility of a denial of service type attack, where a malicious user crafts a message containing a very large number of message attachments. From the 3.3.4 and 3.2.11 releases, a default limit of 50 message attachments is enforced. This is configurable via the message property "attachment-max-count". **CVE ID : CVE-2019-12406**	http://cxf.apache.org/security-advisories.data/CVE-2019-12406.txt.asc	A-APA-CXF-271119/3
Improper Authentication	06-11-2019	7.5	Apache CXF before 3.3.4 and 3.2.11 provides all of the components that are required to build a fully fledged OpenId Connect service. There is a vulnerability in the access token services, where it does not validate that the authenticated principal is equal to that of the supplied clientId parameter in the request. If a malicious client was able to somehow steal an authorization code issued to another client, then they could exploit this vulnerability to obtain an access token for the other client. **CVE ID : CVE-2019-12419**	http://cxf.apache.org/security-advisories.data/CVE-2019-12419.txt.asc	A-APA-CXF-271119/4
arrow					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	08-11-2019	5	It was discovered that the C++ implementation (which underlies the R, Python and Ruby implementations) of Apache Arrow 0.14.0 to 0.14.1 had a uninitialized memory bug when building arrays with null values in some cases. This can lead to uninitialized memory being unintentionally shared if Arrow Arrays are transmitted over the wire (for instance with Flight) or persisted in the streaming IPC and file formats. **CVE ID : CVE-2019-12408**	https://lists.apache.org/thread.html/49f067b1c5fb7493d952580f0d2d032819ba351f7a78743c21126269@%3Cdev.arrow.apache.org%3E	A-APA-ARRO-271119/5
NULL Pointer Dereference	08-11-2019	5	While investigating UBSAN errors in https://github.com/apache/arrow/pull/5365 it was discovered Apache Arrow versions 0.12.0 to 0.14.1, left memory Array data uninitialized when reading RLE null data from parquet. This affected the C++, Python, Ruby and R implementations. The uninitialized memory could potentially be shared if are transmitted over the wire (for instance with Flight) or persisted in the streaming IPC and file formats. **CVE ID : CVE-2019-12410**	N/A	A-APA-ARRO-271119/6
ARM					
mbed-mqtt					
Improper	04-11-2019	5	A denial-of-service issue was	https://gith	A-ARM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			discovered in the MQTT library in Arm Mbed OS 2017-11-02. The function readMQTTLenString() is called by the function MQTTDeserialize_publish() to get the length and content of the MQTT topic name. In the function readMQTTLenString(), mqttstring->lenstring.len is a part of user input, which can be manipulated. An attacker can simply change it to a larger value to invalidate the if statement so that the statements inside the if statement are skipped, letting the value of mqttstring->lenstring.data default to zero. Later, curn is accessed, which points to mqttstring->lenstring.data. On an Arm Cortex-M chip, the value at address 0x0 is actually the initialization value for the MSP register. It is highly dependent on the actual firmware. Therefore, the behavior of the program is unpredictable from this time on. **CVE ID : CVE-2019-17210**	ub.com/ARMmbed/mbed-os/issues/11802	MBED-271119/7
Atlassian					
jira					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate	N/A	A-ATL-JIRA-271119/8

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**		
confluence					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server /	N/A	A-ATL-CONF-271119/9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**		
bitbucket					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**	N/A	A-ATL-BITB-271119/10
crowd					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior	N/A	A-ATL-CROW-271119/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**		
jira_service_desk					
Incorrect Authorization	07-11-2019	4.3	The Customer Context Filter in Atlassian Jira Service Desk Server and Jira Service Desk Data Center before 3.9.17, from 3.10.0 before 3.16.10, from 4.0.0 before 4.2.6, from 4.3.0 before 4.3.5, from 4.4.0 before 4.4.3, and from 4.5.0 before 4.5.1 allows remote attackers with portal access to view arbitrary issues in Jira Service Desk projects via authorization bypass. Note that when the 'Anyone can email the service desk or raise a request in the portal'	N/A	A-ATL-JIRA-271119/12

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			setting is enabled, an attacker can grant themselves portal access, allowing them to exploit the vulnerability. **CVE ID : CVE-2019-15003**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-11-2019	4.3	The Customer Context Filter in Atlassian Jira Service Desk Server and Jira Service Desk Data Center before 3.9.17, from 3.10.0 before 3.16.10, from 4.0.0 before 4.2.6, from 4.3.0 before 4.3.5, from 4.4.0 before 4.4.3, and from 4.5.0 before 4.5.1 allows remote attackers with portal access to view arbitrary issues in Jira Service Desk projects via a path traversal vulnerability. Note that when the 'Anyone can email the service desk or raise a request in the portal' setting is enabled, an attacker can grant themselves portal access, allowing them to exploit the vulnerability. **CVE ID : CVE-2019-15004**	N/A	A-ATL-JIRA-271119/13
troubleshooting_and_support					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration	N/A	A-ATL-TROU-271119/14

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**		
bamboo					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before	N/A	A-ATL-BAMB-271119/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.10.2. **CVE ID : CVE-2019-15005**		
crucible					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**	N/A	A-ATL-CRUC-271119/16
fisheye					
Missing Authorization	08-11-2019	4	The Atlassian Troubleshooting and Support Tools plugin prior to version 1.17.2 allows an unprivileged user to initiate periodic log scans and send the results to a user-specified email address due to a missing authorization	N/A	A-ATL-FISH-271119/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check. The email message may contain configuration information about the application that the plugin is installed into. A vulnerable version of the plugin is included with Bitbucket Server / Data Center before 6.6.0, Confluence Server / Data Center before 7.0.1, Jira Server / Data Center before 8.3.2, Crowd / Crowd Data Center before 3.6.0, Fisheye before 4.7.2, Crucible before 4.7.2, and Bamboo before 6.10.2. **CVE ID : CVE-2019-15005**		
auo					
sunveillance_monitoring_system_\&_data_recorder					
Unrestricted Upload of File with Dangerous Type	12-11-2019	7.5	An issue was discovered in Picture_Manage_mvc.aspx in AUO SunVeillance Monitoring System before v1.1.9e. There is an incorrect access control vulnerability that can allow an unauthenticated user to upload files via a modified authority parameter. **CVE ID : CVE-2019-12719**	N/A	A-AUO-SUNV-271119/18
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-11-2019	5	AUO SunVeillance Monitoring System before v1.1.9e is vulnerable to mvc_send_mail.aspx (MailAdd parameter) SQL Injection. An Attacker can carry a SQL Injection payload to the server, allowing the attacker to read	N/A	A-AUO-SUNV-271119/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged data. This also affects the picture_manage_mvc.aspx plant_no parameter, the swapdl_mvc.aspx plant_no parameter, and the account_management.aspx Text_Postal_Code and Text_Dis_Code parameters. **CVE ID : CVE-2019-12720**		
Avast					
antivirus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	A Cross Site Scripting (XSS) issue exists in Avast AntiVirus (Free, Internet Security, and Premiere Edition) 19.3.2369 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name. **CVE ID : CVE-2019-18653**	N/A	A-AVA-ANTI-271119/20
AVG					
anti-virus					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	A Cross Site Scripting (XSS) issue exists in AVG AntiVirus (Internet Security Edition) 19.3.3084 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name. **CVE ID : CVE-2019-18654**	N/A	A-AVG-ANTI-271119/21
Broadcom					
brocade_sannav					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Through Log Files	08-11-2019	2.1	Brocade SANnav versions before v2.0, logs plain text database connection password while triggering support save. **CVE ID : CVE-2019-16210**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-869	A-BRO-BROC-271119/22
Use of Insufficiently Random Values	08-11-2019	4.3	A vulnerability, in Brocade SANnav versions before v2.0, could allow remote attackers to brute-force a valid session ID. The vulnerability is due to an insufficiently random session ID for several post-authentication actions in the SANnav portal. **CVE ID : CVE-2019-16205**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-864	A-BRO-BROC-271119/23
Information Exposure Through Log Files	08-11-2019	2.1	The authentication mechanism, in Brocade SANnav versions before v2.0, logs plaintext account credentials at the ?trace? and the 'debug' logging level; which could allow a local authenticated attacker to access sensitive information. **CVE ID : CVE-2019-16206**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-865	A-BRO-BROC-271119/24
Use of Hard-coded Credentials	08-11-2019	4.6	Brocade SANnav versions before v2.0 use a hard-coded password, which could allow local authenticated attackers	https://www.broadcom.com/support/fibre-	A-BRO-BROC-271119/25

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to access a back-end database and gain privileges. **CVE ID : CVE-2019-16207**	channel-networking/security-advisories/brocade-security-advisory-2019-866	
Use of a Broken or Risky Cryptographic Algorithm	08-11-2019	5	Password-based encryption (PBE) algorithm, of Brocade SANnav versions before v2.0, has a weakness in generating cryptographic keys that may allow an attacker to decrypt passwords used with several services (Radius, TACAS, etc.). **CVE ID : CVE-2019-16208**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-867	A-BRO-BROC-271119/26
Improper Certificate Validation	08-11-2019	5.8	A vulnerability, in The ReportsTrustManager class of Brocade SANnav versions before v2.0, could allow an attacker to perform a man-in-the-middle attack against Secure Sockets Layer(SSL)connections. **CVE ID : CVE-2019-16209**	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-868	A-BRO-BROC-271119/27
Centrify					
authentication_service					
Deserialization of Untrusted Data	05-11-2019	5.1	The Windows component of Centrify Authentication and Privilege Elevation Services 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.5.0, 3.5.1 (18.8), 3.5.2 (18.11), and 3.6.0 (19.6) does not	https://centrify.force.com/support/Article/KB-22420-Centrify-	A-CEN-AUTH-271119/28

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle an unspecified exception during use of partially trusted assemblies to serialize input data, which allows attackers to execute arbitrary code inside the Centrify process via (1) a crafted application that makes a pipe connection to the process and sends malicious serialized data or (2) a crafted Microsoft Management Console snap-in control file. **CVE ID : CVE-2019-18631**	Agent-for-Windows-Remote-Code-Execution-Vulnerability	
privilege_elevation_service					
Deserialization of Untrusted Data	05-11-2019	5.1	The Windows component of Centrify Authentication and Privilege Elevation Services 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.5.0, 3.5.1 (18.8), 3.5.2 (18.11), and 3.6.0 (19.6) does not properly handle an unspecified exception during use of partially trusted assemblies to serialize input data, which allows attackers to execute arbitrary code inside the Centrify process via (1) a crafted application that makes a pipe connection to the process and sends malicious serialized data or (2) a crafted Microsoft Management Console snap-in control file. **CVE ID : CVE-2019-18631**	https://centrify.force.com/support/Article/KB-22420-Centrify-Agent-for-Windows-Remote-Code-Execution-Vulnerability	A-CEN-PRIV-271119/29

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Ceph					
ceph					
Uncontrolled Resource Consumption	08-11-2019	5	A flaw was found in the Ceph RGW configuration with Beast as the front end handling client requests. An unauthenticated attacker could crash the Ceph RGW server by sending valid HTTP headers and terminating the connection, resulting in a remote denial of service for Ceph RGW clients. **CVE ID : CVE-2019-10222**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10222	A-CEP-CEPH-271119/30
certify					
infrastructure_services					
Deserialization of Untrusted Data	05-11-2019	5.1	The Windows component of Centrify Authentication and Privilege Elevation Services 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.5.0, 3.5.1 (18.8), 3.5.2 (18.11), and 3.6.0 (19.6) does not properly handle an unspecified exception during use of partially trusted assemblies to serialize input data, which allows attackers to execute arbitrary code inside the Centrify process via (1) a crafted application that makes a pipe connection to the process and sends malicious serialized data or (2) a crafted Microsoft Management Console snap-in control file. **CVE ID : CVE-2019-18631**	https://centrify.force.com/support/Article/KB-22420-Centrify-Agent-for-Windows-Remote-Code-Execution-Vulnerability	A-CER-INFR-271119/31

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
chartkick					
chartkick.js					
Improper Input Validation	11-11-2019	7.5	Chartkick.js 3.1.0 through 3.1.3, as used in the Chartkick gem before 3.3.0 for Ruby, allows prototype pollution. **CVE ID : CVE-2019-18841**	https://github.com/ankane/chartkick/commit/b810936bbf687bc74c5b6dba72d2397a399885fa	A-CHA-CHAR-271119/32
Cisco					
firepower_services_software_for_asa					
Improper Authentication	05-11-2019	5	A vulnerability in the stream reassembly component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper reassembly of traffic streams. An attacker could exploit this vulnerability by sending crafted streams through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1978**	N/A	A-CIS-FIRE-271119/33
Improper Authenticati	05-11-2019	5	A vulnerability in the protocol detection	N/A	A-CIS-FIRE-271119/34

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper detection of the initial use of a protocol on a nonstandard port. An attacker could exploit this vulnerability by sending traffic on a nonstandard port for the protocol in use through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. Once the initial protocol flow on the nonstandard port is detected, future flows on the nonstandard port will be successfully detected and handled as configured by the applied policy. **CVE ID : CVE-2019-1980**		
Improper Authenticati on	05-11-2019	5	A vulnerability in the normalization functionality of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow	N/A	A-CIS-FIRE-271119/35

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to insufficient normalization of a text-based payload. An attacker could exploit this vulnerability by sending traffic that contains specifically obfuscated payloads through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious payloads to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1981**		
Incorrect Default Permissions	05-11-2019	5	A vulnerability in the HTTP traffic filtering component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper handling of HTTP requests, including those communicated over a secure HTTPS connection, that contain maliciously crafted headers. An attacker could exploit this vulnerability by sending malicious requests to an affected device. An exploit could allow the attacker to bypass filtering	N/A	A-CIS-FIRE-271119/36

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and deliver malicious requests to protected systems, allowing attackers to deliver malicious content that would otherwise be blocked. **CVE ID : CVE-2019-1982**		
firepower_management_center					
Improper Authentication	05-11-2019	5	A vulnerability in the stream reassembly component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper reassembly of traffic streams. An attacker could exploit this vulnerability by sending crafted streams through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1978**	N/A	A-CIS-FIRE-271119/37
Improper Authentication	05-11-2019	5	A vulnerability in the protocol detection component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center	N/A	A-CIS-FIRE-271119/38

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper detection of the initial use of a protocol on a nonstandard port. An attacker could exploit this vulnerability by sending traffic on a nonstandard port for the protocol in use through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. Once the initial protocol flow on the nonstandard port is detected, future flows on the nonstandard port will be successfully detected and handled as configured by the applied policy. **CVE ID : CVE-2019-1980**		
Improper Authentication	05-11-2019	5	A vulnerability in the normalization functionality of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to insufficient normalization of a text-based payload. An	N/A	A-CIS-FIRE-271119/39

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending traffic that contains specifically obfuscated payloads through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious payloads to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1981**		
Incorrect Default Permissions	05-11-2019	5	A vulnerability in the HTTP traffic filtering component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper handling of HTTP requests, including those communicated over a secure HTTPS connection, that contain maliciously crafted headers. An attacker could exploit this vulnerability by sending malicious requests to an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems, allowing attackers to deliver malicious content that would otherwise be	N/A	A-CIS-FIRE-271119/40

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			blocked. **CVE ID : CVE-2019-1982**		
firepower_threat_defense					
Improper Authentication	05-11-2019	5	A vulnerability in the stream reassembly component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper reassembly of traffic streams. An attacker could exploit this vulnerability by sending crafted streams through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1978**	N/A	A-CIS-FIRE-271119/41
Improper Authentication	05-11-2019	5	A vulnerability in the protocol detection component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to	N/A	A-CIS-FIRE-271119/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improper detection of the initial use of a protocol on a nonstandard port. An attacker could exploit this vulnerability by sending traffic on a nonstandard port for the protocol in use through an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems that would otherwise be blocked. Once the initial protocol flow on the nonstandard port is detected, future flows on the nonstandard port will be successfully detected and handled as configured by the applied policy. **CVE ID : CVE-2019-1980**		
Improper Authentication	05-11-2019	5	A vulnerability in the normalization functionality of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to insufficient normalization of a text-based payload. An attacker could exploit this vulnerability by sending traffic that contains specifically obfuscated payloads through an affected	N/A	A-CIS-FIRE-271119/43

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. An exploit could allow the attacker to bypass filtering and deliver malicious payloads to protected systems that would otherwise be blocked. **CVE ID : CVE-2019-1981**		
Incorrect Default Permissions	05-11-2019	5	A vulnerability in the HTTP traffic filtering component of Cisco Firepower Threat Defense Software, Cisco FirePOWER Services Software for ASA, and Cisco Firepower Management Center Software could allow an unauthenticated, remote attacker to bypass filtering protections. The vulnerability is due to improper handling of HTTP requests, including those communicated over a secure HTTPS connection, that contain maliciously crafted headers. An attacker could exploit this vulnerability by sending malicious requests to an affected device. An exploit could allow the attacker to bypass filtering and deliver malicious requests to protected systems, allowing attackers to deliver malicious content that would otherwise be blocked. **CVE ID : CVE-2019-1982**	N/A	A-CIS-FIRE-271119/44
enterprise_chat_and_email					
Information	05-11-2019	4.3	A vulnerability in the HTTP API of Cisco Enterprise Chat	N/A	A-CIS-ENTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			and Email could allow an unauthenticated, remote attacker to download files attached through chat sessions. The vulnerability is due to insufficient authentication mechanisms on the file download function of the API. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to download files that other users attach through the chat feature. This vulnerability affects versions prior to 12.0(1)ES1. **CVE ID : CVE-2019-1877**		271119/45
telepresence_advanced_media_gateway					
Improper Input Validation	05-11-2019	6.8	A vulnerability in the web application of Cisco TelePresence Advanced Media Gateway could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to the lack of input validation in the web application. An attacker could exploit this vulnerability by sending a crafted authenticated HTTP request to the device. An exploit could allow the attacker to stop services on an affected device. The device may become	N/A	A-CIS-TELE-271119/46

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inoperable and results in a denial of service (DoS) condition. **CVE ID : CVE-2019-15966**		
Clamav					
clamav					
Improper Resource Shutdown or Release	05-11-2019	5	ClamAV versions prior to 0.101.3 are susceptible to a zip bomb vulnerability where an unauthenticated attacker can cause a denial of service condition by sending crafted messages to an affected system. **CVE ID : CVE-2019-12625**	N/A	A-CLA-CLAM-271119/47
Out-of-bounds Read	05-11-2019	5	ClamAV versions prior to 0.101.2 are susceptible to a denial of service (DoS) vulnerability. An out-of-bounds heap read condition may occur when scanning PE files. An example is Windows EXE and DLL files that have been packed using Aspack as a result of inadequate bound-checking. **CVE ID : CVE-2019-1789**	N/A	A-CLA-CLAM-271119/48
djvulibre_project					
djvulibre					
NULL Pointer Dereference	07-11-2019	5	DjVuLibre 3.5.27 has a NULL pointer dereference in the function DJVU::filter_fv at IW44EncodeCodec.cpp. **CVE ID : CVE-2019-18804**	N/A	A-DJV-DJVU-271119/49
Drupal					
svg_sanitizer					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	11-11-2019	5	A Denial Of Service vulnerability exists in the SVG Sanitizer module through 8.x-1.0-alpha1 for Drupal because access to external resources with an SVG use element is mishandled. **CVE ID : CVE-2019-18856**	N/A	A-DRU-SVG_-271119/50
energycap					
energycap					
Improper Privilege Management	08-11-2019	7.5	Escalation of privileges in EnergyCAP 7 through 7.5.6 allows an attacker to access data. If an unauthenticated user clicks on a link on the public dashboard, the resource opens in EnergyCAP with access rights matching the user who created the dashboard. **CVE ID : CVE-2019-18623**	https://energycap.freshdesk.com/helpdesk/attachments/31016649523, https://energycap.freshdesk.com/support/solutions/articles/31000152837-2019-october-24-security-incident-notification-issue-with-public-dashboards-found-and-resolved	A-ENE-ENER-271119/51
enghouse					
web_chat					
Improper Input	13-11-2019	4	An issue was discovered in Enghouse Web Chat	N/A	A-ENG-WEB_-271119/52

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			6.1.300.31 and 6.2.284.34. A user is allowed to send an archive of their chat log to an email address specified at the beginning of the chat (where the user enters in their name and e-mail address). This POST request can be modified to change the message as well as the end recipient of the message. The e-mail address will have the same domain name and user as the product allotted. This can be used in phishing campaigns against users on the same domain. **CVE ID : CVE-2019-16949**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	4.3	An XSS issue was discovered in Enghouse Web Chat 6.1.300.31 and 6.2.284.34. The QueueName parameter of a GET request allows for insertion of user-supplied JavaScript. **CVE ID : CVE-2019-16950**	N/A	A-ENG-WEB_-271119/53
Information Exposure	13-11-2019	5	A remote file include (RFI) issue was discovered in Enghouse Web Chat 6.2.284.34. One can replace the localhost attribute with one's own domain name. When the product calls this domain after the POST request is sent, it retrieves an attacker's data and displays it. Also worth mentioning is the amount of information sent in the request from this product to	N/A	A-ENG-WEB_-271119/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker: it reveals information the public should not have. This includes pathnames and internal ip addresses. **CVE ID : CVE-2019-16951**		
Enghouseinteractive					
web_chat					
Server-Side Request Forgery (SSRF)	13-11-2019	7.5	An SSRF issue was discovered in Enghouse Web Chat 6.1.300.31. In any POST request, one can replace the port number at WebServiceLocation=http://localhost:8085/UCWebServices/ with a range of ports to determine what is visible on the internal network (as opposed to what general web traffic would see on the product's host). The response from open ports is different than from closed ports. The product does not allow one to change the protocol: anything except http(s) will throw an error; however, it is the type of error that allows one to determine if a port is open or not. **CVE ID : CVE-2019-16948**	N/A	A-ENG-WEB_-271119/55
envoyproxy					
envoy					
Loop with Unreachable Exit Condition ('Infinite	11-11-2019	5	Envoy 1.12.0 allows a remote denial of service because of resource loops, as demonstrated by a single idle TCP connection being	https://github.com/envoyproxy/envoy/security/advisorie	A-ENV-ENVO-271119/56

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			able to keep a worker thread in an infinite busy loop when continue_on_listener_filters_timeout is used." **CVE ID : CVE-2019-18836**	s/GHSA-3xvf-4396-cj46	
eximioussoft					
logo_designer					
Out-of-bounds Write	07-11-2019	2.1	Eximious Logo Designer 3.82 has a User Mode Write AV starting at ExiVectorRender!StrokeText_Blend+0x00000000000003a7. **CVE ID : CVE-2019-18819**	N/A	A-EXI-LOGO-271119/57
Out-of-bounds Write	07-11-2019	2.1	Eximious Logo Designer 3.82 has Heap Corruption starting at ntdll!RtlpNtMakeTemporaryKey+0x0000000000001a78. **CVE ID : CVE-2019-18820**	N/A	A-EXI-LOGO-271119/58
Out-of-bounds Write	07-11-2019	1.9	Eximious Logo Designer 3.82 has a User Mode Write AV starting at ExiCustomPathLib!ExiCustomPathLib::CGradientColorsProfile::BuildGradientColorsTable+0x0000000000000053. **CVE ID : CVE-2019-18821**	N/A	A-EXI-LOGO-271119/59
eyecomms					
eyecms					
Improper Input Validation	07-11-2019	4	An Insecure Direct Object Reference (IDOR) vulnerability in eyecomms eyeCMS through 2019-10-15 allows any candidate to change other candidates'	N/A	A-EYE-EYEC-271119/60

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			personal information (first name, last name, email, CV, phone number, and all other personal information) by changing the value of the candidate id (the id parameter). **CVE ID : CVE-2019-17604**		
Incorrect Authorization	07-11-2019	6.5	A mass assignment vulnerability in eyecomms eyeCMS through 2019-10-15 allows any candidate to take over another candidate's account (by also exploiting CVE-2019-17604) via a modified candidate id and an additional password parameter. The outcome is that the password of this other candidate is changed. **CVE ID : CVE-2019-17605**	N/A	A-EYE-EYEC-271119/61
F5					
big-ip_access_policy_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/62
big-ip_advanced_firewall_manager					
Improper Neutralization of Input	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-	https://support.f5.com/csp/article	A-F5-BIG--271119/63

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	/K22441651	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-11-2019	4	On BIG-IP AFM 15.0.0-15.0.1, 14.0.0-14.1.2, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, a vulnerability in the AFM configuration utility may allow any authenticated BIG-IP user to run an SQL injection attack. **CVE ID : CVE-2019-6658**	https://support.f5.com/csp/article/K21121741	A-F5-BIG--271119/64
big-ip_analytics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/65
big-ip_application_acceleration_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/66

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configuration utility. **CVE ID : CVE-2019-6657**		
big-ip_application_security_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/67
big-ip_domain_name_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/68
big-ip_edge_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/69

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
big-ip_fraud_protection_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/70
big-ip_global_traffic_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/71
big-ip_link_controller					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/72
big-ip_local_traffic_manager					
Improper	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1,	https://sup	A-F5-BIG--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	port.f5.com/csp/article/K22441651	271119/73
big-ip_policy_enforcement_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/74
big-ip_webaccelerator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility. **CVE ID : CVE-2019-6657**	https://support.f5.com/csp/article/K22441651	A-F5-BIG--271119/75
Fedoraproject					
389_directory_server					
Use After Free	08-11-2019	3.5	A flaw was found in the 'deref' plugin of 389-ds-base	https://bugzilla.redhat.	A-FED-389_-271119/76

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			where it could use the 'search' permission to display attribute values. In some configurations, this could allow an authenticated attacker to view private attributes, such as password hashes. **CVE ID : CVE-2019-14824**	com/show_bug.cgi?id=CVE-2019-14824	
forcepoint					
security_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-11-2019	4.3	It has been reported that XSS is possible in Forcepoint Email Security, versions 8.5 and 8.5.3. It is strongly recommended that you apply the relevant hotfix in order to remediate this issue. **CVE ID : CVE-2019-6142**	https://support.forcepoint.com/KBArticle?id=000017691	A-FOR-SECU-271119/77
email_security					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-11-2019	4.3	It has been reported that XSS is possible in Forcepoint Email Security, versions 8.5 and 8.5.3. It is strongly recommended that you apply the relevant hotfix in order to remediate this issue. **CVE ID : CVE-2019-6142**	https://support.forcepoint.com/KBArticle?id=000017691	A-FOR-EMAI-271119/78
fudforum					
fudforum					
Improper Neutralization of Special Elements used in an OS	13-11-2019	8.5	FUDForum 3.0.9 is vulnerable to Stored XSS via the nlogin parameter. This may result in remote code execution. An attacker can use a user account to fully	N/A	A-FUD-FUDF-271119/79

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			compromise the system using a POST request. When the admin visits the user information, the payload will execute. This will allow for PHP files to be written to the web root, and for code to execute on the remote server. **CVE ID : CVE-2019-18839**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12-11-2019	8.5	FUDForum 3.0.9 is vulnerable to Stored XSS via the User-Agent HTTP header. This may result in remote code execution. An attacker can use a user account to fully compromise the system via a GET request. When the admin visits user information under "User Manager" in the control panel, the payload will execute. This will allow for PHP files to be written to the web root, and for code to execute on the remote server. The problem is in admsession.php and admuser.php. **CVE ID : CVE-2019-18873**	N/A	A-FUD-FUDF-271119/80
gatech					
computing_for_good's_basic_laboratory_information_system					
Improper Authentication	06-11-2019	5	Computing For Good's Basic Laboratory Information System (also known as C4G BLIS) version 3.5 and earlier suffers from an instance of CWE-284, "Improper Access Control." As a result, an	N/A	A-GAT-COMP-271119/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated user may enumerate the user names and facility names in use on a particular installation. **CVE ID : CVE-2019-5643**		
getigniteup					
igniteup					
Improper Input Validation	12-11-2019	6.4	includes/class-coming-soon-creator.php in the igniteup plugin through 3.4 for WordPress allows unauthenticated arbitrary file deletion. **CVE ID : CVE-2019-17234**	N/A	A-GET-IGNI-271119/82
Information Exposure	12-11-2019	5	includes/class-coming-soon-creator.php in the igniteup plugin through 3.4 for WordPress allows information disclosure. **CVE ID : CVE-2019-17235**	N/A	A-GET-IGNI-271119/83
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	4.3	includes/class-coming-soon-creator.php in the igniteup plugin through 3.4 for WordPress is vulnerable to stored XSS. **CVE ID : CVE-2019-17236**	N/A	A-GET-IGNI-271119/84
Cross-Site Request Forgery (CSRF)	12-11-2019	6.8	includes/class-coming-soon-creator.php in the igniteup plugin through 3.4 for WordPress allows CSRF. **CVE ID : CVE-2019-17237**	N/A	A-GET-IGNI-271119/85
GNU					
mailutils					
Improper Privilege	11-11-2019	4.6	maidag in GNU Mailutils before 3.8 is installed setuid	N/A	A-GNU-MAIL-271119/86

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			and allows local privilege escalation in the url mode. **CVE ID : CVE-2019-18862**		
helm					
helm					
Improper Link Resolution Before File Access ('Link Following')	12-11-2019	7.5	In Helm 2.x before 2.15.2, commands that deal with loading a chart as a directory or packaging a chart provide an opportunity for a maliciously designed chart to include sensitive content such as /etc/passwd, or to execute a denial of service (DoS) via a special file such as /dev/urandom, via symlinks. No version of Tiller is known to be impacted. This is a client-only issue. **CVE ID : CVE-2019-18658**	N/A	A-HEL-HELM-271119/87
Hibernate					
hibernate-validator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-11-2019	4.3	A vulnerability was found in Hibernate-Validator. The SafeHtml validator annotation fails to properly sanitize payloads consisting of potentially malicious code in HTML comments and instructions. This vulnerability can result in an XSS attack. **CVE ID : CVE-2019-10219**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10219	A-HIB-HIBE-271119/88
Huawei					
manageone					
Out-of-	13-11-2019	5	Gauss100 OLTP database in	N/A	A-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			ManageOne with versions of 6.5.0 have an out-of-bounds read vulnerability due to the insufficient checks of the specific packet length. Attackers can construct invalid packets to attack the active and standby communication channels. Successful exploit of this vulnerability could allow the attacker to crash the database on the standby node. **CVE ID : CVE-2019-5289**		MANA-271119/89
IBM					
cognos_controller					
Information Exposure	09-11-2019	4	IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, and 10.4.1 could allow an authenticated user to obtain sensitive information due to easy to guess session identifier names. IBM X-Force ID: 162658. **CVE ID : CVE-2019-4411**	https://www.ibm.com/support/pages/node/1086123	A-IBM-COGN-271119/90
Information Exposure	09-11-2019	5	IBM Cognos Controller stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 162659. **CVE ID : CVE-2019-4412**	https://www.ibm.com/support/pages/node/1086123	A-IBM-COGN-271119/91
spectrum_protect_plus					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	12-11-2019	3.6	IBM Spectrum Protect Plus 10.1.0 through 10.1.4 uses insecure file permissions on restored files and directories in Windows which could allow a local user to obtain sensitive information or perform unauthorized actions. IBM X-Force ID: 170963. **CVE ID : CVE-2019-4652**	https://www.ibm.com/support/pages/node/1105683	A-IBM-SPEC-271119/92
cognos_analytics					
Information Exposure	09-11-2019	4	IBM Cognos Analytics 11.0 and 11.1 could reveal sensitive information to an authenticated user that could be used in future attacks against the system. IBM X-Force ID: 161271. **CVE ID : CVE-2019-4334**	https://www.ibm.com/support/pages/node/1074144	A-IBM-COGN-271119/93
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-11-2019	4.3	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170881. **CVE ID : CVE-2019-4645**	https://www.ibm.com/support/pages/node/1074144	A-IBM-COGN-271119/94
qradar_advisor_with_watson					
Improper Input Validation	09-11-2019	4	IBM QRadar Advisor 1.0.0 through 2.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass	https://www.ibm.com/support/pages/node/1	A-IBM-QRAD-271119/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 166205. **CVE ID : CVE-2019-4556**	102443	
qradar_security_information_and_event_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-11-2019	3.5	IBM QRadar 7.3.0 to 7.3.2 Patch 4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163618. **CVE ID : CVE-2019-4454**	https://www.ibm.com/support/pages/node/1103499	A-IBM-QRAD-271119/96
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-11-2019	3.5	IBM QRadar 7.3.0 to 7.3.2 Patch 4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163779. **CVE ID : CVE-2019-4470**	https://www.ibm.com/support/pages/node/1103517	A-IBM-QRAD-271119/97
Incorrect Authorization	09-11-2019	4	IBM QRadar 7.3.0 to 7.3.2 Patch 4 is vulnerable to incorrect authorization in some components which could allow an authenticated user to obtain sensitive	https://www.ibm.com/support/pages/node/1103931	A-IBM-QRAD-271119/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information. IBM X-Force ID: 164430. **CVE ID : CVE-2019-4509**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-11-2019	4.3	IBM QRadar 7.3.0 to 7.3.2 Patch 4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 167239. **CVE ID : CVE-2019-4581**	https://www.ibm.com/support/pages/node/1103373	A-IBM-QRAD-271119/99
Imagemagick					
imagemagick					
Improper Input Validation	11-11-2019	4.3	ImageMagick before 7.0.9-0 allows remote attackers to cause a denial of service because XML_PARSE_HUGE is not properly restricted in coders/svg.c, related to SVG and libxml2. **CVE ID : CVE-2019-18853**	N/A	A-IMA-IMAG-271119/100
infosysta					
in-app_\&_desktop_notifications					
Information Exposure	01-11-2019	5	An issue was discovered in the Infosysta "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects without authentication/authorization via the plugins/servlet/nfj/ProjectFilter?searchQuery= URI.	N/A	A-INF-IN-A-271119/101

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-16908		
Information Exposure	01-11-2019	4	An issue was discovered in the Infosysta "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects (with authentication as a Jira user, but without authorization for specific projects) via the plugins/servlet/nfj/NotificationSettings URI. **CVE ID : CVE-2019-16909**	N/A	A-INF-IN-A-271119/102
Intercom					
intercom					
Information Exposure	12-11-2019	5	The Intercom plugin through 1.2.1 for WordPress leaks a Slack Access Token in source code. An attacker can obtain a lot of information about the victim's Slack (channels, members, etc.). **CVE ID : CVE-2019-14365**	N/A	A-INT-INTE-271119/103
Investintech					
able2extract					
Out-of-bounds Write	05-11-2019	6.8	An exploitable memory corruption vulnerability exists in Investintech Able2Extract Professional 14.0.7 x64. A specially crafted BMP file can cause an out-of-bounds memory write, allowing a potential attacker to execute arbitrary code on the victim machine. Can trigger this vulnerability by sending the user a specially crafted BMP file.	N/A	A-INV-ABLE-271119/104

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-5088		
Out-of-bounds Write	05-11-2019	6.8	An exploitable memory corruption vulnerability exists in Investintech Able2Extract Professional 4.0.7 x64. A specially crafted JPEG file can cause an out-of-bounds memory write, allowing an attacker to execute arbitrary code on the victim machine. An attacker could exploit a vulnerability by providing the user with a specially crafted JPEG file. **CVE ID : CVE-2019-5089**	N/A	A-INV-ABLE-271119/105
ISC					
dhcpd					
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensuse-security-announce/2019-10/msg00048.html	A-ISC-DHCP-271119/106

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**		
bind					
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensus	A-ISC-BIND-271119/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**	e-security-announce/2019-10/msg00048.html	
isl					
arp-guard					
Improper Neutralization of Special Elements used in an	04-11-2019	7.5	A SQL injection vulnerability in a /login/forgot1 POST request in ARP-GUARD 4.0.0-5 allows unauthenticated remote	N/A	A-ISL-ARP--271119/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			attackers to execute arbitrary SQL commands via the user_id parameter. **CVE ID : CVE-2019-18663**		
istio					
istio					
Loop with Unreachable Exit Condition ('Infinite Loop')	12-11-2019	5	Istio 1.3.x before 1.3.5 allows Denial of Service because continue_on_listener_filters_timeout is set to True, a related issue to CVE-2019-18836. **CVE ID : CVE-2019-18817**	N/A	A-IST-ISTI-271119/109
Loop with Unreachable Exit Condition ('Infinite Loop')	11-11-2019	5	Envoy 1.12.0 allows a remote denial of service because of resource loops, as demonstrated by a single idle TCP connection being able to keep a worker thread in an infinite busy loop when continue_on_listener_filters_timeout is used." **CVE ID : CVE-2019-18836**	https://github.com/envoyproxy/envoy/security/advisories/GHSA-3xvf-4396-cj46	A-IST-ISTI-271119/110
jitbit					
.net_forum					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	3.5	A cross-site scripting (XSS) vulnerability in Jitbit .NET Forum (aka ASP.NET forum) 8.3.8 allows remote attackers to inject arbitrary web script or HTML via the gravatar URL parameter. **CVE ID : CVE-2019-18636**	N/A	A-JIT-.NET-271119/111
Joomla					
joomla\!					
Cross-Site Request	06-11-2019	6.8	An issue was discovered in Joomla! before 3.9.13. A	N/A	A-JOO-JOOM-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			missing token check in com_template causes a CSRF vulnerability. **CVE ID : CVE-2019-18650**		271119/112
Missing Authorization	06-11-2019	5	An issue was discovered in Joomla! before 3.9.13. A missing access check in the phputf8 mapping files could lead to a path disclosure. **CVE ID : CVE-2019-18674**	N/A	A-JOO-JOOM-271119/113
json-jwt_project					
json-jwt					
Improper Input Validation	12-11-2019	5	The json-jwt gem before 1.11.0 for Ruby lacks an element count during the splitting of a JWE string. **CVE ID : CVE-2019-18848**	N/A	A-JSO-JSON-271119/114
Kubernetes					
kube-state-metrics					
Information Exposure	05-11-2019	4	A security issue was discovered in the kube-state-metrics versions v1.7.0 and v1.7.1. An experimental feature was added to the v1.7.0 release that enabled annotations to be exposed as metrics. By default, the kube-state-metrics metrics only expose metadata about Secrets. However, a combination of the default `kubectl` behavior and this new feature can cause the entire secret content to end up in metric labels thus inadvertently exposing the secret content in metrics. This feature has been	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10223	A-KUB-KUBE-271119/115

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reverted and released as the v1.7.2 release. If you are running the v1.7.0 or v1.7.1 release, please upgrade to the v1.7.2 release as soon as possible. **CVE ID : CVE-2019-10223**		
lavalite					
lavalite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	4.3	XSS exists in Lavalite CMS 5.7 via the admin/profile name or designation field. **CVE ID : CVE-2019-18883**	N/A	A-LAV-LAVA-271119/116
Leadtools					
leadtools					
Out-of-bounds Write	06-11-2019	6.8	An exploitable heap out-of-bounds write vulnerability exists in the TIF-parsing functionality of LEADTOOLS 20. A specially crafted TIF image can cause an offset beyond the bounds of a heap allocation to be written, potentially resulting in code execution. An attacker can specially craft a TIF image to trigger this vulnerability. **CVE ID : CVE-2019-5084**	N/A	A-LEA-LEAD-271119/117
Integer Overflow or Wraparound	06-11-2019	6.8	An exploitable integer underflow vulnerability exists in the CMP-parsing functionality of LEADTOOLS 20. A specially crafted CMP image file can cause an	N/A	A-LEA-LEAD-271119/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			integer underflow, potentially resulting in code execution. An attacker can specially craft a CMP image to trigger this vulnerability. **CVE ID : CVE-2019-5099**		
Integer Overflow or Wraparound	06-11-2019	6.8	An exploitable integer overflow vulnerability exists in the BMP header parsing functionality of LEADTOOLS 20. A specially crafted BMP image file can cause an integer overflow, potentially resulting in code execution. An attacker can specially craft a BMP image to trigger this vulnerability. **CVE ID : CVE-2019-5100**	N/A	A-LEA-LEAD-271119/119
Out-of-bounds Write	06-11-2019	6.8	An exploitable heap overflow vulnerability exists in the JPEG2000 parsing functionality of LEADTOOLS 20. A specially crafted J2K image file can cause an out of bounds write of a heap buffer, potentially resulting in code execution. An attack can specially craft a J2K image to trigger this vulnerability. **CVE ID : CVE-2019-5125**	N/A	A-LEA-LEAD-271119/120
lightbend					
play_framework					
Insufficiently Protected Credentials	05-11-2019	4.3	An issue was discovered in Lightbend Play Framework 2.5.x through 2.6.23. When configured to make requests using an authenticated HTTP proxy, play-ws may	https://www.playframework.com/security/vulnerability/CVE-2019-	A-LIG-PLAY-271119/121

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sometimes, typically under high load, when connecting to a target host using https, expose the proxy credentials to the target host. **CVE ID : CVE-2019-17598**	17598-PlayWSHttpConnectAuthorizationHeaders	
Magento					
magento					
N/A	05-11-2019	5.5	An arbitrary file deletion vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. An authenticated users can manipulate the design layout update feature. **CVE ID : CVE-2019-8090**	N/A	A-MAG-MAGE-271119/122
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 1 prior to 1.9.4.3 and 1.14.4.3. An authenticated admin user with privileges to access product attributes can leverage layout updates to trigger remote code execution. **CVE ID : CVE-2019-8091**	N/A	A-MAG-MAGE-271119/123
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-11-2019	3.5	A reflected cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code via email template preview. **CVE ID : CVE-2019-8092**	N/A	A-MAG-MAGE-271119/124
Unrestricted	05-11-2019	6.5	An arbitrary file access	N/A	A-MAG-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Upload of File with Dangerous Type			vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can leverage file upload controller for downloadable products to read/delete an arbitary files. **CVE ID : CVE-2019-8093**		MAGE-271119/125
Improper Input Validation	05-11-2019	5.5	An arbitrary file deletion vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with export data transfer privileges can craft a request to perform arbitrary file deletion. **CVE ID : CVE-2019-8107**	N/A	A-MAG-MAGE-271119/126
Improper Authenticati on	05-11-2019	4	Insecure authentication and session management vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can manipulate session validation setting for a storefront that leads to insecure authentication and session management. **CVE ID : CVE-2019-8108**	N/A	A-MAG-MAGE-271119/127
Cross-Site Request Forgery (CSRF)	05-11-2019	6	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can craft a malicious CSRF payload that can result in arbitrary command	N/A	A-MAG-MAGE-271119/128

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2019-8109**		
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can leverage email templates hierarchy to manipulate the interceptor class in a way that allows an attacker to execute arbitrary code. **CVE ID : CVE-2019-8110**	N/A	A-MAG-MAGE-271119/129
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can leverage plugin functionality related to email templates to manipulate the interceptor class in a way that allows an attacker to execute arbitrary code. **CVE ID : CVE-2019-8111**	N/A	A-MAG-MAGE-271119/130
Insufficient Verification of Data Authenticity	05-11-2019	5	A security bypass vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An unauthenticated user can bypass the email confirmation mechanism via GET request that captures relevant account data obtained from the POST response related to new user creation. **CVE ID : CVE-2019-8112**	N/A	A-MAG-MAGE-271119/131

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	05-11-2019	5	Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1 uses cryptographically weak random number generator to brute-force the confirmation code for customer registration. **CVE ID : CVE-2019-8113**	N/A	A-MAG-MAGE-271119/132
Unrestricted Upload of File with Dangerous Type	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 1 prior to 1.9.4.3 and 1.14.4.3, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with admin privileges to import features can execute arbitrary code via crafted configuration archive file upload. **CVE ID : CVE-2019-8114**	N/A	A-MAG-MAGE-271119/133
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-11-2019	3.5	A reflected cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated admin user can inject arbitrary JavaScript code when adding an image for during simple product creation. **CVE ID : CVE-2019-8115**	N/A	A-MAG-MAGE-271119/134
Improper Authentication	05-11-2019	5	Insecure authentication and session management vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An unauthenticated	N/A	A-MAG-MAGE-271119/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user can leverage a guest session id value following a successful login to gain access to customer account index page. **CVE ID : CVE-2019-8116**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticates user can inject arbitrary JavaScript code via product view id specification. **CVE ID : CVE-2019-8117**	N/A	A-MAG-MAGE-271119/136
Cleartext Storage of Sensitive Information	05-11-2019	5	Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 uses weak cryptographic function to store the failed login attempts for customer accounts. **CVE ID : CVE-2019-8118**	N/A	A-MAG-MAGE-271119/137
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. An authenticated admin user with import product privileges can delete files through bulk product import and inject code into XSLT file. The combination of these manipulations can lead to remote code execution. **CVE ID : CVE-2019-8119**	N/A	A-MAG-MAGE-271119/138
Improper Neutralizati	05-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in	N/A	A-MAG-MAGE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. An authenticated user can inject arbitrary Javascript code by manipulating section of a POST request related to customer's email address. **CVE ID : CVE-2019-8120**		271119/139
N/A	05-11-2019	7.5	An insecure component vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. Magento 2 codebase leveraged outdated versions of JS libraries (Bootstrap, jquery, Knockout) with known security vulnerabilities. **CVE ID : CVE-2019-8121**	N/A	A-MAG-MAGE-271119/140
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. An authenticated user with privileges to create products can craft custom layout update and use import product functionality to enable remote code execution. **CVE ID : CVE-2019-8122**	N/A	A-MAG-MAGE-271119/141
Improper Input Validation	05-11-2019	5	An insufficient logging and monitoring vulnerability exists in Magento 1 prior to 1.9.4.3 and 1.14.4.3, Magento	N/A	A-MAG-MAGE-271119/142

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
			2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. The logging feature required for effective monitoring did not contain sufficent data to effectively track configuration changes. **CVE ID : CVE-2019-8123**		
Insufficient Verification of Data Authenticity	05-11-2019	5	An insufficient logging and monitoring vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. Failure to track admin actions related to design configuration could lead to repudiation attacks. **CVE ID : CVE-2019-8124**	N/A	A-MAG-MAGE-271119/143
Improper Input Validation	05-11-2019	6.5	A remote code execution vulnerability exists in Magento 1 prior to 1.9.x and 1.14.x. An authenticated admin user can modify configuration parameters via crafted support configuration. The modification can lead to remote code execution. **CVE ID : CVE-2019-8125**	N/A	A-MAG-MAGE-271119/144
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	05-11-2019	4	An XML entity injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated admin user can craft document type definition for an XML representing XML layout. The crafted	N/A	A-MAG-MAGE-271119/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			document type definition and XML layout allow processing of external entities which can lead to information disclosure. **CVE ID : CVE-2019-8126**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-11-2019	6.5	A SQL injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with privileges to an account with Newsletter Template editing permission could exfiltrate the Admin login data, and reset their password, effectively performing a privilege escalation. **CVE ID : CVE-2019-8127**	N/A	A-MAG-MAGE-271119/146
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can exploit it by injecting malicious Javascript into the name of main website. **CVE ID : CVE-2019-8128**	N/A	A-MAG-MAGE-271119/147
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can exploit it by injecting an embedded expression into a translation. **CVE ID : CVE-2019-8129**	N/A	A-MAG-MAGE-271119/148

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	6.5	A SQL injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. A user with store manipulation privileges can execute arbitrary SQL queries by getting access to the database connection through group instance in email templates. **CVE ID : CVE-2019-8130**	N/A	A-MAG-MAGE-271119/149
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code into code field of an inventory source. **CVE ID : CVE-2019-8131**	N/A	A-MAG-MAGE-271119/150
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can craft malicious payload in the template Name field for Email template in the "Design Configuration" dashboard. **CVE ID : CVE-2019-8132**	N/A	A-MAG-MAGE-271119/151
Improper Input Validation	06-11-2019	4	A security bypass vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. A user with privileges to generate sitemaps can bypass	N/A	A-MAG-MAGE-271119/152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration that restricts directory access. The bypass allows overwrite of a subset of configuration files which can lead to denial of service. **CVE ID : CVE-2019-8133**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	6.5	A SQL injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. A user with marketing privileges can execute arbitrary SQL queries in the database when accessing email template variables. **CVE ID : CVE-2019-8134**	N/A	A-MAG-MAGE-271119/153
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	7.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. Dependency injection through Symphony framework allows service identifiers to be derived from user controlled data, which can lead to remote code execution. **CVE ID : CVE-2019-8135**	N/A	A-MAG-MAGE-271119/154
N/A	06-11-2019	7.5	An insecure component vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. Magento 2 codebase leveraged outdated versions of HTTP specification abstraction implemented in symphony component. **CVE ID : CVE-2019-8136**	N/A	A-MAG-MAGE-271119/155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with privileges to manipulate CMS section of the website can trigger remote code execution via custom layout update. **CVE ID : CVE-2019-8137**	N/A	A-MAG-MAGE-271119/156
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can execute arbitrary JavaScript code by providing arbitrary API endpoint that will not be chcecked by sale pickup event. **CVE ID : CVE-2019-8138**	N/A	A-MAG-MAGE-271119/157
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary Javascript code into the dynamic block when invoking page builder on a product. **CVE ID : CVE-2019-8139**	N/A	A-MAG-MAGE-271119/158
Unrestricted Upload of File with Dangerous Type	06-11-2019	4	An unrestricted file upload vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated admin user can manipulate the Synchronization feature	N/A	A-MAG-MAGE-271119/159

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in the Media File Storage of the database to transform uploaded JPEG file into a PHP file. **CVE ID : CVE-2019-8140**		
Deserialization of Untrusted Data	06-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.19, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3. An authenticated user with administrative privileges (system level import) can execute arbitrary code through a Phar deserialization vulnerability in the import functionality. **CVE ID : CVE-2019-8141**	N/A	A-MAG-MAGE-271119/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code via title of an order when configuring sales payment methods for a store. **CVE ID : CVE-2019-8142**	N/A	A-MAG-MAGE-271119/161
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	4	A SQL injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with access to email templates can send malicious SQL queries and obtain access to sensitive information stored in the database.	N/A	A-MAG-MAGE-271119/162

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-8143		
Improper Input Validation	06-11-2019	7.5	A remote code execution vulnerability exists in Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An unauthenticated user can insert a malicious payload through PageBuilder template methods. **CVE ID : CVE-2019-8144**	N/A	A-MAG-MAGE-271119/163
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code into the attribute set name when listing the products. **CVE ID : CVE-2019-8145**	N/A	A-MAG-MAGE-271119/164
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code when adding a new customer attribute for stores. **CVE ID : CVE-2019-8146**	N/A	A-MAG-MAGE-271119/165
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can inject arbitrary JavaScript code via customer attribute label.	N/A	A-MAG-MAGE-271119/166

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-8147		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated admin user can inject arbitrary JavaScript code when creating a content page via page builder. **CVE ID : CVE-2019-8148**	N/A	A-MAG-MAGE-271119/167
Session Fixation	06-11-2019	7.5	Insecure authentication and session management vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An unauthenticated user can append arbitrary session id that will not be invalidated by subsequent authentication. **CVE ID : CVE-2019-8149**	N/A	A-MAG-MAGE-271119/168
Improper Input Validation	06-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with privileges to manipulate layouts and images can insert a malicious payload into the page layout. **CVE ID : CVE-2019-8150**	N/A	A-MAG-MAGE-271119/169
Server-Side Request Forgery (SSRF)	06-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with admin privileges to manipulate shippment	N/A	A-MAG-MAGE-271119/170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			settings can execute arbitrary code through server-side request forgery due to unsafe handling of a carrier gateway. **CVE ID : CVE-2019-8151**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in in Magento 1 prior to 1.9.4.3 and 1.14.4.3, Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with access to the wysiwyg editor can abuse the blockDirective() function and inject malicious javascript in the cache of the admin dashboard. **CVE ID : CVE-2019-8152**	N/A	A-MAG-MAGE-271119/171
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	4.3	A mitigation bypass to prevent cross-site scripting (XSS) exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. Successful exploitation of this vulnerability would result in an attacker being able to bypass the `escapeURL()` function and execute a malicious XSS payload. **CVE ID : CVE-2019-8153**	N/A	A-MAG-MAGE-271119/172
Improper Input Validation	06-11-2019	6.5	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with privileges to	N/A	A-MAG-MAGE-271119/173

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			modify product catalogs can trigger PHP file inclusion through a crafted XML file that specifies product design update. **CVE ID : CVE-2019-8154**		
Information Exposure	06-11-2019	5	Magento prior to 1.9.4.3 and prior to 1.14.4.3 included a user's CSRF token in the URL of a GET request. This could be exploited by an attacker with access to network traffic to perform unauthorized actions. **CVE ID : CVE-2019-8155**	N/A	A-MAG-MAGE-271119/174
Server-Side Request Forgery (SSRF)	06-11-2019	6.5	A server-side request forgery (SSRF) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with admin privileges to modify store configurations can manipulate the connector api endpoint to enable remote code execution. **CVE ID : CVE-2019-8156**	N/A	A-MAG-MAGE-271119/175
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	A stored cross-site scripting (XSS) vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user can manipulate downloadable link and cause an invocation of error handling that acceses user input without sanitization. **CVE ID : CVE-2019-8157**	N/A	A-MAG-MAGE-271119/176

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
XML Injection (aka Blind XPath Injection)	06-11-2019	7.5	An XPath entity injection vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An attacker can craft a GET request to page cache block rendering module that gets passed to XML data processing engine without validation. The crafted key/value GET request data allows an attacker to limited access to underlying XML data. **CVE ID : CVE-2019-8158**	N/A	A-MAG-MAGE-271119/177
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-11-2019	9	A remote code execution vulnerability exists in Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1. An authenticated user with system data manipulation privileges can execute aribitrary code through arbitrary file deletion and OS command injection. **CVE ID : CVE-2019-8159**	N/A	A-MAG-MAGE-271119/178
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	In Magento prior to 1.9.4.3 and Magento prior to 1.14.4.3, an authenticated user with limited administrative privileges can inject arbitrary JavaScript code via import / export functionality when creating profile action XML. **CVE ID : CVE-2019-8227**	N/A	A-MAG-MAGE-271119/179
Improper Neutralizati	06-11-2019	3.5	in Magento prior to 1.9.4.3 and Magento prior to	N/A	A-MAG-MAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			1.14.4.3, an authenticated user with limited administrative privileges can inject arbitrary JavaScript code into transactional email page when creating a new email template or editing existing email template. **CVE ID : CVE-2019-8228**		271119/180
Improper Input Validation	06-11-2019	6.5	In Magento prior to 1.9.4.3, and Magento prior to 1.14.4.3, an authenticated user with administrative privileges to edit product attributes can execute arbitrary code through crafted layout updates. **CVE ID : CVE-2019-8229**	N/A	A-MAG-MAGE-271119/181
Improper Input Validation	06-11-2019	6.5	In Magentoprior to 1.9.4.3, and Magento prior to 1.14.4.3, an authenticated user with administrative privileges to edit configuration settings can execute arbitrary code through a crafted support/output path. **CVE ID : CVE-2019-8230**	N/A	A-MAG-MAGE-271119/182
Improper Input Validation	06-11-2019	6.5	In Magento to 1.9.4.3 and Magento prior to 1.14.4.3, an authenticated user with administrative privileges for editing attribute sets can execute arbitrary code through custom layout modification. **CVE ID : CVE-2019-8231**	N/A	A-MAG-MAGE-271119/183
Improper Input	06-11-2019	6	In Magento prior to 1.9.4.3, Magento prior to 1.14.4.3,	N/A	A-MAG-MAGE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Magento 2.2 prior to 2.2.10, and Magento 2.3 prior to 2.3.3 or 2.3.2-p1, an authenticated user with administrative privileges for the import feature can execute arbitrary code through a race condition that allows webserver configuration file modification. **CVE ID : CVE-2019-8232**		271119/184
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	4.3	In Magento 2.2 prior to 2.2.10, Magento 2.3 prior to 2.3.3 or 2.3.2-p1, an unauthenticated user can inject arbitrary JavaScript code as a result of the sanitization engine ignoring HTML comments. **CVE ID : CVE-2019-8233**	N/A	A-MAG-MAGE-271119/185
Matrix					
synapse					
Improper Verification of Cryptographic Signature	08-11-2019	7.5	Matrix Synapse before 1.5.0 mishandles signature checking on some federation APIs. Events sent over /send_join, /send_leave, and /invite may not be correctly signed, or may not come from the expected servers. **CVE ID : CVE-2019-18835**	N/A	A-MAT-SYNA-271119/186
Mcafee					
advanced_threat_defense					
Information Exposure	13-11-2019	4	Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows	N/A	A-MCA-ADVA-271119/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote authenticated attackers to gain access to hashed credentials via carefully constructed POST request extracting incorrectly recorded data from log files. **CVE ID : CVE-2019-3649**		
Information Exposure	13-11-2019	4	Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD prior to 4.8 allows remote authenticated attackers to gain access to the atduser credentials via carefully constructed GET request extracting insecurely information stored in the database. **CVE ID : CVE-2019-3650**	N/A	A-MCA-ADVA-271119/188
Information Exposure	13-11-2019	6.5	Information Disclosure vulnerability in McAfee Advanced Threat Defense (ATD prior to 4.8 allows remote authenticated attackers to gain access to ePO as an administrator via using the atduser credentials, which were too permissive. **CVE ID : CVE-2019-3651**	N/A	A-MCA-ADVA-271119/189
Improper Neutralization of Special Elements in Output Used by a Downstream	13-11-2019	6.5	Improper Neutralization of HTTP requests in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to execute commands on the server remotely via carefully	https://kc.mcafee.com/corporate/index?page=content&id=SB10304	A-MCA-ADVA-271119/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			constructed HTTP requests. **CVE ID : CVE-2019-3660**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-11-2019	6.5	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to execute database commands via carefully constructed time based payloads. **CVE ID : CVE-2019-3661**	N/A	A-MCA-ADVA-271119/191
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14-11-2019	4	Path Traversal: '/absolute/pathname/here' vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows remote authenticated attacker to gain unintended access to files on the system via carefully constructed HTTP requests. **CVE ID : CVE-2019-3662**	N/A	A-MCA-ADVA-271119/192
Insufficiently Protected Credentials	14-11-2019	2.1	Unprotected Storage of Credentials vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.8 allows local attacker to gain access to the root password via accessing sensitive files on the system. **CVE ID : CVE-2019-3663**	N/A	A-MCA-ADVA-271119/193
threat_intelligence_exchange_server					
Improper Authentication	13-11-2019	3.5	Abuse of Authorization vulnerability in APIs exposed by TIE server in	https://kc.mcafee.com/corporate/	A-MCA-THRE-271119/194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			McAfee Threat Intelligence Exchange Server (TIE Server) 3.0.0 allows remote authenticated users to modify stored reputation data via specially crafted messages. **CVE ID : CVE-2019-3641**	index?page=content&id=SB10303	
Medtronic					
valleylab_exchange_client					
Improper Input Validation	08-11-2019	7.2	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use the descrypt algorithm for OS password hashing. While interactive, network-based logons are disabled, and attackers can use the other vulnerabilities within this report to obtain local shell access and access these hashes. **CVE ID : CVE-2019-13539**	N/A	A-MED-VALL-271119/195
Use of Hard-coded Credentials	08-11-2019	5	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use multiple sets of	N/A	A-MED-VALL-271119/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hard-coded credentials. If discovered, they can be used to read files on the device. **CVE ID : CVE-2019-13543**		
Mesa3d					
mesa					
Incorrect Permission Assignment for Critical Resource	05-11-2019	3.6	An exploitable shared memory permissions vulnerability exists in the functionality of X11 Mesa 3D Graphics Library 19.1.2. An attacker can access the shared memory without any specific permissions to trigger this vulnerability. **CVE ID : CVE-2019-5068**	N/A	A-MES-MESA-271119/197
Microsoft					
azure_stack					
Authentication Bypass by Spoofing	12-11-2019	5	A spoofing vulnerability exists when Azure Stack fails to validate certain requests, aka 'Azure Stack Spoofing Vulnerability'. **CVE ID : CVE-2019-1234**	N/A	A-MIC-AZUR-271119/198
chakracore					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1426**	N/A	A-MIC-CHAK-271119/199

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1427**	N/A	A-MIC-CHAK-271119/200
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429. **CVE ID : CVE-2019-1428**	N/A	A-MIC-CHAK-271119/201
edge					
Improper Input Validation	12-11-2019	4.3	A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls, aka 'Microsoft Edge Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1413**	N/A	A-MIC-EDGE-271119/202
Improper Restriction of Operations	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory	N/A	A-MIC-EDGE-271119/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1426**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1427**	N/A	A-MIC-EDGE-271119/204
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429. **CVE ID : CVE-2019-1428**	N/A	A-MIC-EDGE-271119/205
office					
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft	N/A	A-MIC-OFFI-271119/206

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Office Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1402**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-OFFI-271119/207
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1448**	N/A	A-MIC-OFFI-271119/208
Improper Privilege Managemen t	12-11-2019	10	A security feature bypass vulnerability exists in the way that Office Click-to-Run (C2R) components handle a specially crafted file, which could lead to a standard user, any AppContainer sandbox, and Office LPAC Protected View to escalate privileges to SYSTEM.To exploit this bug, an attacker would have to run a specially crafted file, aka 'Microsoft Office ClickToRun Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1449**	N/A	A-MIC-OFFI-271119/209
Improper Input	12-11-2019	6.8	A security feature bypass vulnerability exists in	N/A	A-MIC-OFFI-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Microsoft Office software by not enforcing macro settings on an Excel document, aka 'Microsoft Office Excel Security Feature Bypass'. **CVE ID : CVE-2019-1457**		271119/210
office_365_proplus					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1448**	N/A	A-MIC-OFFI-271119/211
Improper Privilege Managemen t	12-11-2019	10	A security feature bypass vulnerability exists in the way that Office Click-to-Run (C2R) components handle a specially crafted file, which could lead to a standard user, any AppContainer sandbox, and Office LPAC Protected View to escalate privileges to SYSTEM.To exploit this bug, an attacker would have to run a specially crafted file, aka 'Microsoft Office ClickToRun Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1449**	N/A	A-MIC-OFFI-271119/212
internet_explorer					
Improper Restriction of Operations within the	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code	N/A	A-MIC-INTE-271119/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Execution Vulnerability'. **CVE ID : CVE-2019-1390**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	A-MIC-INTE-271119/214
sharepoint_server					
Improper Input Validation	12-11-2019	4.3	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs.An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka 'Microsoft Office Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1442**	N/A	A-MIC-SHAR-271119/215
Information Exposure	12-11-2019	4	An information disclosure vulnerability exists in Microsoft SharePoint when an attacker uploads a specially crafted file to the SharePoint Server.An authenticated attacker who successfully exploited this vulnerability could potentially leverage SharePoint functionality to obtain SMB hashes.The	N/A	A-MIC-SHAR-271119/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security update addresses the vulnerability by correcting how SharePoint checks file content., aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1443**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-SHAR-271119/217
sharepoint_enterprise_server					
Information Exposure	12-11-2019	4	An information disclosure vulnerability exists in Microsoft SharePoint when an attacker uploads a specially crafted file to the SharePoint Server.An authenticated attacker who successfully exploited this vulnerability could potentially leverage SharePoint functionality to obtain SMB hashes.The security update addresses the vulnerability by correcting how SharePoint checks file content., aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1443**	N/A	A-MIC-SHAR-271119/218
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when	N/A	A-MIC-SHAR-271119/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**		
office_online_server					
Improper Input Validation	12-11-2019	5.8	A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications handlers correctly, aka 'Microsoft Office Online Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1447. **CVE ID : CVE-2019-1445**	N/A	A-MIC-OFFI-271119/220
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-OFFI-271119/221
Improper Input Validation	12-11-2019	5.8	A spoofing vulnerability exists when Office Online does not validate origin in cross-origin communications handlers correctly, aka 'Microsoft Office Online Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1445. **CVE ID : CVE-2019-1447**	N/A	A-MIC-OFFI-271119/222
exchange_server					
Deserialization of	12-11-2019	7.5	A remote code execution vulnerability exists in	N/A	A-MIC-EXCH-271119/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			Microsoft Exchange through the deserialization of metadata via PowerShell, aka 'Microsoft Exchange Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1373**		
sharepoint_foundation					
Information Exposure	12-11-2019	4	An information disclosure vulnerability exists in Microsoft SharePoint when an attacker uploads a specially crafted file to the SharePoint Server.An authenticated attacker who successfully exploited this vulnerability could potentially leverage SharePoint functionality to obtain SMB hashes.The security update addresses the vulnerability by correcting how SharePoint checks file content., aka 'Microsoft SharePoint Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1443**	N/A	A-MIC-SHAR-271119/224
excel					
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-EXCE-271119/225
Improper Restriction	12-11-2019	9.3	A remote code execution vulnerability exists in	N/A	A-MIC-EXCE-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1448**		271119/226
excel_services					
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-EXCE-271119/227
office_365					
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Microsoft Office software when the software fails to properly handle objects in memory, aka 'Microsoft Office Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1402**	N/A	A-MIC-OFFI-271119/228
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1446**	N/A	A-MIC-OFFI-271119/229
open_enclave_software_development_kit					
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when affected Open Enclave SDK	N/A	A-MIC-OPEN-271119/230

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1370**		
microstrategy					
microstrategy_library					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-11-2019	4.3	Microstrategy Library in MicroStrategy before 2019 before 11.1.3 has reflected XSS. **CVE ID : CVE-2019-18957**	N/A	A-MIC-MICR-271119/231
nicehash					
miner					
Improper Input Validation	06-11-2019	5	An issue was discovered in NiceHash Miner before 2.0.3.0. A missing rate limit while adding a wallet via Email address allows remote attackers to submit a large number of email addresses to identify valid ones. By exploiting this vulnerability with CVE-2019-6122 (Username Enumeration) an adversary can enumerate a large number of valid users' Email addresses. **CVE ID : CVE-2019-6120**	N/A	A-NIC-MINE-271119/232
Missing Authorization	06-11-2019	4.3	An issue was discovered in NiceHash Miner before 2.0.3.0. Missing Authorization allows an adversary to can gain access	N/A	A-NIC-MINE-271119/233

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to a miner's information about such as his recent payments, unclaimed Balance, Old Balance (at the time of December 2017 breach) , Projected payout, Mining stats like profitability, Efficiency, Number of workers, etc.. A valid Email address is required in order to retrieve this Information. **CVE ID : CVE-2019-6121**		
Information Exposure	06-11-2019	4.3	A Username Enumeration via Error Message issue was discovered in NiceHash Miner before 2.0.3.0 because an "EMAIL DOES NOT EXIST" error message occurs whenever a submitted email address is incorrect, but there is a different error message for invalid credentials with a correct email address. **CVE ID : CVE-2019-6122**	N/A	A-NIC-MINE-271119/234
Nvidia					
geforce_experience					
Improper Input Validation	09-11-2019	4.6	NVIDIA GeForce Experience, all versions prior to 3.20.1, contains a vulnerability in the Downloader component in which a user with local system access can craft input that may allow malicious files to be downloaded and saved. This behavior may lead to code execution, denial of service, or	https://nvidia.custhelp.com/app/answers/detail/a_id/4860	A-NVI-GEFO-271119/235

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2019-5689**		
Untrusted Search Path	12-11-2019	4.4	NVIDIA GeForce Experience (prior to 3.20.1) and Windows GPU Display Driver (all versions) contains a vulnerability in the local service provider component in which an attacker with local system and privileged access can incorrectly load Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution. **CVE ID : CVE-2019-5695**	https://nvidia.custhelp.com/app/answers/detail/a_id/4860, https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-GEFO-271119/236
Untrusted Search Path	09-11-2019	4.4	NVIDIA GeForce Experience, all versions prior to 3.20.1, contains a vulnerability when GameStream is enabled in which an attacker with local system access can load the Intel graphics driver DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service, information disclosure, or escalation of privileges through code execution. **CVE ID : CVE-2019-5701**	https://nvidia.custhelp.com/app/answers/detail/a_id/4860	A-NVI-GEFO-271119/237
gpu_driver					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the size of an input buffer is not validated, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2019-5690**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-GPU_-271119/238
NULL Pointer Dereference	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which a NULL pointer is dereferenced, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2019-5691**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-GPU_-271119/239
Improper Input Validation	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the product uses untrusted input when calculating or using an array index, which may lead to escalation of privileges or denial of service. **CVE ID : CVE-2019-5692**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-GPU_-271119/240
Access of Uninitialized Pointer	09-11-2019	4.9	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer	https://nvidia.custhelp.com/app/answers/det	A-NVI-GPU_-271119/241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(nvlddmkm.sys) in which the program accesses or uses a pointer that has not been initialized, which may lead to denial of service. **CVE ID : CVE-2019-5693**	ail/a_id/4907	
Untrusted Search Path	09-11-2019	4.4	NVIDIA Windows GPU Display Driver, R390 driver version, contains a vulnerability in NVIDIA Control Panel in which it incorrectly loads Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution. The attacker requires local system access. **CVE ID : CVE-2019-5694**	N/A	A-NVI-GPU_-271119/242
Untrusted Search Path	12-11-2019	4.4	NVIDIA GeForce Experience (prior to 3.20.1) and Windows GPU Display Driver (all versions) contains a vulnerability in the local service provider component in which an attacker with local system and privileged access can incorrectly load Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure	https://nvidia.custhelp.com/app/answers/detail/a_id/4860, https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-GPU_-271119/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through code execution. **CVE ID : CVE-2019-5695**		
virtual_gpu_manager					
Out-of-bounds Read	09-11-2019	2.1	NVIDIA Virtual GPU Manager, all versions, contains a vulnerability in which the provision of an incorrectly sized buffer by a guest VM leads to GPU out-of-bound access, which may lead to a denial of service. **CVE ID : CVE-2019-5696**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-VIRT-271119/244
Incorrect Authorization	09-11-2019	3.6	NVIDIA Virtual GPU Manager, all versions, contains a vulnerability in which it may grant a guest access to memory that it does not own, which may lead to information disclosure or denial of service. **CVE ID : CVE-2019-5697**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-VIRT-271119/245
Improper Input Validation	09-11-2019	2.1	NVIDIA Virtual GPU Manager, all versions, contains a vulnerability in the vGPU plugin, in which an input index value is incorrectly validated, which may lead to denial of service. **CVE ID : CVE-2019-5698**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	A-NVI-VIRT-271119/246
oneidentity					
cloud_access_manager					
Improper Validation of Integrity Check Value	04-11-2019	4.3	One Identity Cloud Access Manager before 8.1.4 Hotfix 1 allows OTP bypass via vectors involving a man in the middle, the One Identity Defender product, and	https://support.oneidentity.com/cloud-access-manager/kb/311391/	A-ONE-CLOU-271119/247

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			replacing a failed SAML response with a successful SAML response. **CVE ID : CVE-2019-13496**	cloud-access-manager-8-1-4-hotfix-1	
Cross-Site Request Forgery (CSRF)	04-11-2019	4.3	One Identity Cloud Access Manager before 8.1.4 Hotfix 1 allows CSRF for logout requests. **CVE ID : CVE-2019-13497**	https://support.oneidentity.com/cloud-access-manager/kb/311391/cloud-access-manager-8-1-4-hotfix-1	A-ONE-CLOU-271119/248
Opensuse					
open_build_service					
Improper Certificate Validation	05-11-2019	6.8	Open Build Service before version 0.165.4 diddn't validate TLS certificates for HTTPS connections with the osc client binary **CVE ID : CVE-2019-3685**	https://bugzilla.suse.com/show_bug.cgi?id=1142518	A-OPE-OPEN-271119/249
Oxid-esales					
eshop					
Session Fixation	05-11-2019	6.8	An issue was discovered in OXID eShop 6.x before 6.0.6 and 6.1.x before 6.1.5, OXID eShop Enterprise Edition Version 5.2.x-5.3.x, OXID eShop Professional Edition Version 4.9.x-4.10.x and OXID eShop Community Edition Version: 4.9.x-4.10.x. By using a specially crafted URL, users with administrative rights could unintentionally grant unauthorized users access to	N/A	A-OXI-ESHO-271119/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the admin panel via session fixation. **CVE ID : CVE-2019-17062**		
Parallels					
parallels_plesk_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	4.3	Parallels Plesk Panel 9.5 allows XSS in target/locales/tr-TR/help/index.htm? via the "fileName" parameter. **CVE ID : CVE-2019-18793**	N/A	A-PAR-PARA-271119/251
Pfsense					
pfsense-pkg-freeradius3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-11-2019	4.3	/usr/local/www/freeradius_view_config.php in the freeradius3 package before 0.15.7_3 for pfSense on FreeBSD allows a user with an XSS payload as password or username to execute arbitrary javascript code on a victim browser. **CVE ID : CVE-2019-18667**	N/A	A-PFS-PFSE-271119/252
phantomjs					
phantomjs					
Files or Directories Accessible to External Parties	05-11-2019	5	PhantomJS through 2.1.1 has an arbitrary file read vulnerability, as demonstrated by an XMLHttpRequest for a file:// URI. The vulnerability exists in the page.open() function of the webpage module, which loads a specified URL and calls a given callback. An attacker can supply a	N/A	A-PHA-PHAN-271119/253

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted HTML file, as user input, that allows reading arbitrary files on the filesystem. For example, if page.render() is the function callback, this generates a PDF or an image of the targeted file. NOTE: this product is no longer developed. **CVE ID : CVE-2019-17221**		
Philips					
tasy_emr					
Information Exposure	08-11-2019	5	In Tasy EMR, Tasy WebPortal Versions 3.02.1757 and prior, there is an information exposure vulnerability which may allow a remote attacker to access system and configuration information. **CVE ID : CVE-2019-13557**	N/A	A-PHI-TASY-271119/254
tasy_webportal					
Information Exposure	08-11-2019	5	In Tasy EMR, Tasy WebPortal Versions 3.02.1757 and prior, there is an information exposure vulnerability which may allow a remote attacker to access system and configuration information. **CVE ID : CVE-2019-13557**	N/A	A-PHI-TASY-271119/255
phoenix					
securecore_technology					
Improper Privilege Managemen	13-11-2019	6.8	In Phoenix SCT WinFlash 1.1.12.0 through 1.5.74.0, the included drivers could be used by a malicious	https://www.phoenix.com/content/uploads/S	A-PHO-SECU-271119/256

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			Windows application to gain elevated privileges. Adverse impacts are limited to the Windows environment and there is no known direct impact to the UEFI firmware. This was fixed in late June 2019. **CVE ID : CVE-2019-18279**	ecurity-Newsletter-September-2019.pdf	
phpspreadsheet_project					
phpspreadsheet					
Improper Restriction of XML External Entity Reference ('XXE')	07-11-2019	6.8	PHPOffice PhpSpreadsheet before 1.8.0 has an XXE issue. The XmlScanner decodes the sheet1.xml from an .xlsx to utf-8 if something else than UTF-8 is declared in the header. This was a security measurement to prevent CVE-2018-19277 but the fix is not sufficient. By double-encoding the the xml payload to utf-7 it is possible to bypass the check for the string ?<!ENTITY? and thus allowing for an xml external entity processing (XXE) attack. **CVE ID : CVE-2019-12331**	https://github.com/PHPOffice/PhpSpreadsheet/blob/master/CHANGELOG.md#180---2019-07-01	A-PHP-PHPS-271119/257
popojicms					
popojicms					
URL Redirection to Untrusted Site ('Open Redirect')	07-11-2019	5.8	PopojiCMS 2.0.1 allows refer= Open Redirection. **CVE ID : CVE-2019-18815**	N/A	A-POP-POPO-271119/258
Improper Neutralizati	07-11-2019	4.3	po-admin/route.php?mod=post	N/A	A-POP-POPO-271119/259

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			&act=edit in PopojiCMS 2.0.1 allows post[1][content]= stored XSS. **CVE ID : CVE-2019-18816**		
portainer					
portainer					
Incorrect Permission Assignment for Critical Resource	07-11-2019	9	Portainer before 1.22.1 has Incorrect Access Control (issue 1 of 4). **CVE ID : CVE-2019-16872**	N/A	A-POR-PORT-271119/260
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-11-2019	3.5	Portainer before 1.22.1 has XSS (issue 1 of 2). **CVE ID : CVE-2019-16873**	N/A	A-POR-PORT-271119/261
Incorrect Permission Assignment for Critical Resource	07-11-2019	4	Portainer before 1.22.1 has Incorrect Access Control (issue 2 of 4). **CVE ID : CVE-2019-16874**	N/A	A-POR-PORT-271119/262
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-11-2019	5	Portainer before 1.22.1 allows Directory Traversal. **CVE ID : CVE-2019-16876**	N/A	A-POR-PORT-271119/263
Incorrect Permission Assignment for Critical Resource	07-11-2019	6.5	Portainer before 1.22.1 has Incorrect Access Control (issue 4 of 4). **CVE ID : CVE-2019-16877**	N/A	A-POR-PORT-271119/264

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-11-2019	3.5	Portainer before 1.22.1 has XSS (issue 2 of 2). **CVE ID : CVE-2019-16878**	N/A	A-POR-PORT-271119/265
psutil_project					
psutil					
Double Free	12-11-2019	5	psutil (aka python-psutil) through 5.6.5 can have a double free. This occurs because of refcount mishandling within a while or for loop that converts system data into a Python object. **CVE ID : CVE-2019-18874**	N/A	A-PSU-PSUT-271119/266
Quest					
kace_systems_management_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	4.3	A reflected XSS vulnerability exists in Quest KACE Systems Management Appliance Server Center 9.1.317 affecting the userui/software_library.php component via the PATH_INFO. **CVE ID : CVE-2019-12917**	N/A	A-QUE-KACE-271119/267
Improper Neutralization of Special Elements used in an SQL Command ('SQL	06-11-2019	7.5	Quest KACE Systems Management Appliance Server Center version 9.1.317 is vulnerable to SQL injection. The affected file is software_library.php and affected parameters are order[0][column] and	N/A	A-QUE-KACE-271119/268

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			order[0][dir]. **CVE ID : CVE-2019-12918**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	6.5	Quest KACE Systems Management Appliance Server Center 9.1.317 is vulnerable to SQL injection. An authenticated user has the ability to execute arbitrary commands against the database. The affected component is /userui/ticket_list.php, and affected parameters are order[0][column] and order[0][dir]. **CVE ID : CVE-2019-13076**	N/A	A-QUE-KACE-271119/269
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	4.3	Quest KACE Systems Management Appliance Server Center 9.1.317 has an XSS vulnerability (via the sam_detail_titled.php SAM_TYPE parameter) that allows an attacker to create a malicious link in order to attack authenticated users. **CVE ID : CVE-2019-13077**	N/A	A-QUE-KACE-271119/270
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	6.5	Quest KACE Systems Management Appliance Server Center 9.1.317 is vulnerable to SQL injection. An authenticated user has the ability to execute arbitrary commands against the database. The affected component is /common/user_profile.php. The affected parameter is sort_column. **CVE ID : CVE-2019-13078**	N/A	A-QUE-KACE-271119/271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	6.5	Quest KACE Systems Management Appliance Server Center 9.1.317 is vulnerable to SQL injection. An authenticated user has the ability to execute arbitrary commands against the database. The affected component is /adminui/history_log.php. The affected parameter is TYPE_NAME. **CVE ID : CVE-2019-13079**	N/A	A-QUE-KACE-271119/272
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	Quest KACE Systems Management Appliance Server Center 9.1.317 has an XSS vulnerability (via an SVG image and HTML file) that allows an authenticated user to execute arbitrary JavaScript in an administrator's browser. **CVE ID : CVE-2019-13080**	N/A	A-QUE-KACE-271119/273
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-11-2019	3.5	Quest KACE Systems Management Appliance Server Center 9.1.317 has an XSS vulnerability (via the title field in the /common/ticket_associated_tickets.php service desk ticket functionality) that allows an authenticated user to execute arbitrary JavaScript in a service desk user's browser. **CVE ID : CVE-2019-13081**	N/A	A-QUE-KACE-271119/274
rakuten					
viber					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-11-2019	4.3	Viber through 11.7.0.5 allows a remote attacker who can capture a victim's internet traffic to steal their Viber account, because not all Viber protocol traffic is encrypted. TCP data packet 9 on port 4244 from the victim's device contains cleartext information such as the device model and OS version, IMSI, and 20 bytes of udid in a binary format, which is located at offset 0x14 of this packet. Then, the attacker installs Viber on his device, initiates the registration process for any phone number, but doesn't enter a pin from SMS. Instead, he closes Viber. Next, the attacker rewrites his udid with the victim's udid, modifying the viber_udid file, which is located in the Viber preferences folder. (The udid is stored in a hexadecimal format.) Finally, the attacker starts Viber again and enters the pin from SMS. **CVE ID : CVE-2019-18800**	N/A	A-RAK-VIBE-271119/275
Rapid7					
metasploit					
Incorrect Permission Assignment for Critical Resource	06-11-2019	2.1	Rapid7 Metasploit Pro version 4.16.0-2019081901 and prior suffers from an instance of CWE-732, wherein the unique	https://help.rapid7.com/metasploit/release-notes/?rid=	A-RAP-META-271119/276

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server.key is written to the file system during installation with world-readable permissions. This can allow other users of the same system where Metasploit Pro is installed to intercept otherwise private communications to the Metasploit Pro web interface. **CVE ID : CVE-2019-5642**	4.16.0-2019091001	
ready					
wireless_emergency_alerts					
Use of a Broken or Risky Cryptographic Algorithm	02-11-2019	5	The Wireless Emergency Alerts (WEA) protocol allows remote attackers to spoof a Presidential Alert because cryptographic authentication is not used, as demonstrated by MessageIdentifier 4370 in LTE System Information Block 12 (aka SIB12). NOTE: testing inside an RF-isolated shield box suggested that all LTE phones are affected by design (e.g., use of Android versus iOS does not matter); testing in an open RF environment is, of course, contraindicated. **CVE ID : CVE-2019-18659**	N/A	A-REA-WIRE-271119/277
Redhat					
jboss_data_grid					
Improper Neutralization of Input During Web	08-11-2019	4.3	A vulnerability was found in Hibernate-Validator. The SafeHtml validator annotation fails to properly	https://bugzilla.redhat.com/show_bug.cgi?id=	A-RED-JBOS-271119/278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			sanitize payloads consisting of potentially malicious code in HTML comments and instructions. This vulnerability can result in an XSS attack. **CVE ID : CVE-2019-10219**	CVE-2019-10219	
jboss_fuse					
Improper Input Validation	08-11-2019	4.3	It was found that the Syndesis configuration for Cross-Origin Resource Sharing was set to allow all origins. An attacker could use this lack of protection to conduct phishing attacks and further access unauthorized information. **CVE ID : CVE-2019-14860**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14860	A-RED-JBOS-271119/279
openstack-mistral					
Information Exposure Through Log Files	08-11-2019	2.1	An information-exposure vulnerability was discovered where openstack-mistral's undercloud log files containing clear-text information were made world readable. A malicious system user could exploit this flaw to access sensitive user information. **CVE ID : CVE-2019-3866**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3866	A-RED-OPEN-271119/280
jboss_enterprise_application_platform					
Improper Neutralization of Input During Web Page Generation ('Cross-site	08-11-2019	4.3	A vulnerability was found in Hibernate-Validator. The SafeHtml validator annotation fails to properly sanitize payloads consisting of potentially malicious code in HTML comments and	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10219	A-RED-JBOS-271119/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			instructions. This vulnerability can result in an XSS attack. **CVE ID : CVE-2019-10219**		
single_sign-on					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-11-2019	4.3	A vulnerability was found in Hibernate-Validator. The SafeHtml validator annotation fails to properly sanitize payloads consisting of potentially malicious code in HTML comments and instructions. This vulnerability can result in an XSS attack. **CVE ID : CVE-2019-10219**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10219	A-RED-SING-271119/282
openshift_container_platform					
Information Exposure	05-11-2019	4	A security issue was discovered in the kube-state-metrics versions v1.7.0 and v1.7.1. An experimental feature was added to the v1.7.0 release that enabled annotations to be exposed as metrics. By default, the kube-state-metrics metrics only expose metadata about Secrets. However, a combination of the default `kubectl` behavior and this new feature can cause the entire secret content to end up in metric labels thus inadvertently exposing the secret content in metrics. This feature has been reverted and released as the v1.7.2 release. If you are running the v1.7.0 or v1.7.1	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10223	A-RED-OPEN-271119/283

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			release, please upgrade to the v1.7.2 release as soon as possible. **CVE ID : CVE-2019-10223**		
openstack					
Information Exposure Through Log Files	08-11-2019	2.1	An information-exposure vulnerability was discovered where openstack-mistral's undercloud log files containing clear-text information were made world readable. A malicious system user could exploit this flaw to access sensitive user information. **CVE ID : CVE-2019-3866**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3866	A-RED-OPEN-271119/284
ceph_storage					
Uncontrolled Resource Consumption	08-11-2019	5	A flaw was found in the Ceph RGW configuration with Beast as the front end handling client requests. An unauthenticated attacker could crash the Ceph RGW server by sending valid HTTP headers and terminating the connection, resulting in a remote denial of service for Ceph RGW clients. **CVE ID : CVE-2019-10222**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10222	A-RED-CEPH-271119/285
syndesis					
Improper Input Validation	08-11-2019	4.3	It was found that the Syndesis configuration for Cross-Origin Resource Sharing was set to allow all origins. An attacker could use this lack of protection to conduct phishing attacks and	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14860	A-RED-SYND-271119/286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further access unauthorized information. **CVE ID : CVE-2019-14860**		
safe_svg_project					
safe_svg					
Uncontrolled Recursion	11-11-2019	5	A Denial Of Service vulnerability exists in the safe-svg (aka Safe SVG) plugin through 1.9.4 for WordPress, related to unlimited recursion for a '<use ... xlink:href="#identifier">' substring. **CVE ID : CVE-2019-18854**	N/A	A-SAF-SAFE-271119/287
Improper Input Validation	11-11-2019	5	A Denial Of Service vulnerability exists in the safe-svg (aka Safe SVG) plugin through 1.9.4 for WordPress, related to potentially unwanted elements or attributes. **CVE ID : CVE-2019-18855**	N/A	A-SAF-SAFE-271119/288
salesagility					
suitecrm					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-11-2019	7.5	SuiteCRM 7.10.x versions prior to 7.10.21 and 7.11.x versions prior to 7.11.9 allow SQL Injection. **CVE ID : CVE-2019-18784**	N/A	A-SAL-SUIT-271119/289
Samba					
samba					
Improper	06-11-2019	4.3	A flaw was found in the	https://bug	A-SAM-SAMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user. **CVE ID : CVE-2019-10218**	zilla.redhat.com/show_bug.cgi?id=CVE-2019-10218	271119/290
Weak Password Requirements	06-11-2019	4.9	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks. **CVE ID : CVE-2019-14833**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14833	A-SAM-SAMB-271119/291
NULL Pointer	06-11-2019	4	A flaw was found in samba 4.0.0 before samba 4.9.15	https://bugzilla.redhat.	A-SAM-SAMB-271119/292

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue. **CVE ID : CVE-2019-14847**	com/show_bug.cgi?id=CVE-2019-14847	
SAP					
hana_database					
Improper Input Validation	04-11-2019	5	SAP HANA Database, versions 1.0, 2.0, allows an unauthorized attacker to send a malformed connection request, which crashes the indexserver of an SAP HANA instance, leading to Denial of Service **CVE ID : CVE-2019-0350**	N/A	A-SAP-HANA-271119/293
diagnostics_agent					
Information Exposure	13-11-2019	4	Under certain conditions SAP Data Hub (corrected in DH_Foundation version 2) allows an attacker to access information which would otherwise be restricted. Connection details that are maintained in Connection Manager are visible to users. **CVE ID : CVE-2019-0390**	N/A	A-SAP-DIAG-271119/294
quality_management					
Improper Neutralization of Special Elements used in an SQL Command	13-11-2019	4	An SQL Injection vulnerability in SAP Quality Management (corrected in S4CORE versions 1.0, 1.01, 1.02, 1.03) allows an attacker to carry out targeted database queries	N/A	A-SAP-QUAL-271119/295

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			that can read individual fields of historical inspection results. **CVE ID : CVE-2019-0393**		
netweaver_application_server_java					
Improper Privilege Managemen t	13-11-2019	6.5	An administrator of SAP NetWeaver Application Server Java (J2EE-Framework), (corrected in versions 7.1, 7.2, 7.3, 7.31, 7.4, 7.5), may change privileges for all or some functions in Java Server, and enable users to execute functions, they are not allowed to execute otherwise. **CVE ID : CVE-2019-0389**	N/A	A-SAP-NETW-271119/296
Information Exposure	13-11-2019	4	Under certain conditions SAP NetWeaver AS Java (corrected in 7.10, 7.20, 7.30, 7.31, 7.40, 7.50) allows an attacker to access information which would otherwise be restricted. **CVE ID : CVE-2019-0391**	N/A	A-SAP-NETW-271119/297
enable_now					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	3.5	SAP Enable Now, before version 1908, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0385**	N/A	A-SAP-ENAB-271119/298
businessobjects_business_intelligence_platform					
Improper Neutralizati	13-11-2019	3.5	A Cross-Site Scripting vulnerability exists in SAP	N/A	A-SAP-BUSI-271119/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on of Input During Web Page Generation ('Cross-site Scripting')			BusinessObjects Business Intelligence Platform (Web Intelligence-Publication related pages); corrected in version 4.2. Privileges are required in order to exploit this vulnerability. **CVE ID : CVE-2019-0382**		
Improper Input Validation	13-11-2019	5.5	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), corrected in versions 4.1 and 4.2, does not sufficiently validate an XML document accepted from an untrusted source. An attacker can craft a message that contains malicious elements that will not be correctly filtered by Web Intelligence HTML interface in some specific workflows. **CVE ID : CVE-2019-0396**	N/A	A-SAP-BUSI-271119/300
Sass-lang					
Libsass					
Uncontrolled Recursion	06-11-2019	4.3	LibSass 3.6.1 has uncontrolled recursion in Sass::Eval::operator()(Sass::Binary_Expression*) in eval.cpp. **CVE ID : CVE-2019-18797**	N/A	A-SAS-LIBS-271119/301
Out-of-bounds Read	06-11-2019	4.3	LibSass before 3.6.3 allows a heap-based buffer over-read in Sass::weaveParents in ast_sel_weave.cpp. **CVE ID : CVE-2019-18798**	N/A	A-SAS-LIBS-271119/302
NULL	06-11-2019	4.3	LibSass before 3.6.3 allows a	N/A	A-SAS-LIBS-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			NULL pointer dereference in Sass::Parser::parseCompoundSelector in parser_selectors.cpp. **CVE ID : CVE-2019-18799**		271119/303
secudos					
domos					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-11-2019	3.5	The Log module in SECUDOS DOMOS before 5.6 allows XSS. **CVE ID : CVE-2019-18664**	N/A	A-SEC-DOMO-271119/304
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-11-2019	5	The Log module in SECUDOS DOMOS before 5.6 allows local file inclusion. **CVE ID : CVE-2019-18665**	N/A	A-SEC-DOMO-271119/305
Sibsoft					
xfilesharing					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	13-11-2019	5	SibSoft Xfilesharing through 2.5.1 allows op=page&tmpl=../ directory traversal to read arbitrary files. **CVE ID : CVE-2019-18951**	N/A	A-SIB-XFIL-271119/306
Unrestricted Upload of File with Dangerous Type	13-11-2019	7.5	SibSoft Xfilesharing through 2.5.1 allows cgi-bin/up.cgi arbitrary file upload. This can be combined with CVE-2019-18951 to achieve	N/A	A-SIB-XFIL-271119/307

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote code execution via a .html file, containing short codes, that is served over HTTP. **CVE ID : CVE-2019-18952**		
Simplesamlphp					
simplesamlphp					
Improper Input Validation	07-11-2019	6.5	Rob Richards XmlSecLibs, all versions prior to v3.0.3, as used for example by SimpleSAMLphp, performed incorrect validation of cryptographic signatures in XML messages, allowing an authenticated attacker to impersonate others or elevate privileges by creating a crafted XML message. **CVE ID : CVE-2019-3465**	N/A	A-SIM-SIMP-271119/308
slack					
wp_slacksync					
Information Exposure	12-11-2019	5	WP SlackSync plugin through 1.8.5 for WordPress leaks a Slack Access Token in source code. An attacker can obtain a lot of information about the victim's Slack (channels, members, etc.). **CVE ID : CVE-2019-14366**	N/A	A-SLA-WP_S-271119/309
slack-chat_project					
slack-chat					
Information Exposure	12-11-2019	5	Slack-Chat through 1.5.5 leaks a Slack Access Token in source code. An attacker can obtain a lot of information about the victim's Slack	N/A	A-SLA-SLAC-271119/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(channels, members, etc.). **CVE ID : CVE-2019-14367**		
Sonatype					
nexus_repository_manager					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-11-2019	9	There is an OS Command Injection in Nexus Repository Manager <= 2.14.14 (bypass CVE-2019-5475) that could allow an attacker a Remote Code Execution (RCE). All instances using CommandLineExecutor.java with user-supplied data is vulnerable, such as the Yum Configuration Capability. **CVE ID : CVE-2019-15588**	https://support.sonatype.com/hc/en-us/articles/360033490774-CVE-2019-5475-Nexus-Repository-Manager-2-OS-Command-Injection-2019-08-09	A-SON-NEXU-271119/311
strapi					
strapi					
Weak Password Recovery Mechanism for Forgotten Password	07-11-2019	5	strapi before 3.0.0-beta.17.5 mishandles password resets within packages/strapi-admin/controllers/Auth.js and packages/strapi-plugin-users-permissions/controllers/Auth.js. **CVE ID : CVE-2019-18818**	N/A	A-STR-STRA-271119/312
sudo_project					
sudo					
Concurrent Execution using Shared Resource with	04-11-2019	6.9	** DISPUTED ** Sudo through 1.8.29 allows local users to escalate to root if they have write access to file descriptor 3 of the sudo process. This occurs because	N/A	A-SUD-SUDO-271119/313

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			of a race condition between determining a uid, and the setresuid and openat system calls. The attacker can write "ALL ALL=(ALL) NOPASSWD:ALL" to /proc/#####/fd/3 at a time when Sudo is prompting for a password. NOTE: This has been disputed due to the way Linux /proc works. It has been argued that writing to /proc/#####/fd/3 would only be viable if you had permission to write to /etc/sudoers. Even with write permission to /proc/#####/fd/3, it would not help you write to /etc/sudoers. **CVE ID : CVE-2019-18684**		
svg-sanitizer_project					
svg-sanitizer					
Improper Input Validation	11-11-2019	5	darylldoyle svg-sanitizer before 0.12.0 mishandles script and data values in attributes, as demonstrated by unexpected whitespace such as in the javascript :alert substring. **CVE ID : CVE-2019-18857**	N/A	A-SVG-SVG--271119/314
Symantec					
sonar					
Incorrect Default Permissions	01-11-2019	4.1	The Symantec SONAR component, prior to 12.0.2, may be susceptible to a tamper protection bypass vulnerability which could	https://support.symantec.com/us/en/article.SYMSA1494.	A-SYM-SONA-271119/315

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially allow an attacker to circumvent the existing tamper protection in use on the resident system. **CVE ID : CVE-2019-12752**	html	
systematic					
iris_webforms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	12-11-2019	5	Systematic IRIS WebForms 5.4 is vulnerable to directory traversal. By manipulating variables that reference files with ../ (and variations), it is possible to list all the directories and check if a particular file exists. **CVE ID : CVE-2019-18924**	N/A	A-SYS-IRIS-271119/316
Improper Authenticati on	12-11-2019	7.5	Systematic IRIS WebForms 5.4 and its functionalities can be accessed and used without any form of authentication. **CVE ID : CVE-2019-18925**	N/A	A-SYS-IRIS-271119/317
systematicinc					
iris_standards_management					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	4.3	Systematic IRIS Standards Management (ISM) v2.1 SP1 89 is vulnerable to unauthenticated reflected Cross Site Scripting (XSS). A user input (related to dialog information) is reflected directly in the web page, allowing a malicious user to conduct a Cross Site Scripting attack against users of the application. **CVE ID : CVE-2019-18926**	N/A	A-SYS-IRIS-271119/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Tibco					
ebx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	4.3	The Web server component of TIBCO Software Inc.'s TIBCO EBX contains multiple vulnerabilities that theoretically allow authenticated users to perform stored cross-site scripting (XSS) attacks, and unauthenticated users to perform reflected cross-site scripting attacks. Affected releases are TIBCO Software Inc.'s TIBCO EBX: versions up to and including 5.8.1.fixR, versions 5.9.3, 5.9.4, 5.9.5, and 5.9.6. **CVE ID : CVE-2019-17330**	N/A	A-TIB-EBX-271119/319
ebx_add-ons					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	3.5	The Data Exchange Web Interface component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains a vulnerability that theoretically allows authenticated users to perform stored cross-site scripting (XSS) attacks. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions up to and including 3.20.13, version 4.1.0. **CVE ID : CVE-2019-17331**	N/A	A-TIB-EBX_-271119/320
Improper Neutralization of Input During Web	12-11-2019	4.3	The Digital Asset Manager Web Interface component of TIBCO Software Inc.'s TIBCO EBX Add-ons contains a	N/A	A-TIB-EBX_-271119/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			vulnerability that theoretically allows authenticated users to perform stored cross-site scripting (XSS) attacks. Affected releases are TIBCO Software Inc.'s TIBCO EBX Add-ons: versions up to and including 3.20.13, versions 4.1.0, 4.2.0, 4.2.1, and 4.2.2. **CVE ID : CVE-2019-17332**		
Tmaxsoft					
jeus					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-11-2019	6.5	JEUS 7 Fix#0~5 and JEUS 8Fix#0~1 versions contains a directory traversal vulnerability caused by improper input parameter check when uploading installation file in administration web page. That leads remote attacker to execute arbitrary code via uploaded file. **CVE ID : CVE-2019-17327**	N/A	A-TMA-JEUS-271119/322
tnef_project					
tnef					
Out-of-bounds Read	11-11-2019	4.3	In tnef before 1.4.18, an attacker may be able to write to the victim's .ssh/authorized_keys file via an e-mail message with a crafted winmail.dat application/ms-tnef attachment, because of a heap-based buffer over-read involving strdup. **CVE ID : CVE-2019-18849**	N/A	A-TNE-TNEF-271119/323

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
untangle					
ng_firewall					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	14-11-2019	6.5	The Untangle NG firewall 14.2.0 is vulnerable to authenticated inline-query SQL injection within the timeDataDynamicColumn parameter when logged in as an admin user. **CVE ID : CVE-2019-18646**	N/A	A-UNT-NG_F-271119/324
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	14-11-2019	9	The Untangle NG firewall 14.2.0 is vulnerable to an authenticated command injection when logged in as an admin user. **CVE ID : CVE-2019-18647**	N/A	A-UNT-NG_F-271119/325
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-11-2019	3.5	When logged in as an admin user, the Untangle NG firewall 14.2.0 is vulnerable to reflected XSS at multiple places and specific user input fields. **CVE ID : CVE-2019-18648**	N/A	A-UNT-NG_F-271119/326
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-11-2019	3.5	When logged in as an admin user, the Title input field (under Reports) within Untangle NG firewall 14.2.0 is vulnerable to stored XSS. **CVE ID : CVE-2019-18649**	N/A	A-UNT-NG_F-271119/327
Veritas					
access					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**	N/A	A-VER-ACCE-271119/328
access_appliance					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between	N/A	A-VER-ACCE-271119/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**		
flex_appliance					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**	N/A	A-VER-FLEX-271119/330
infoscale					
Improper	05-11-2019	10	An arbitrary command	N/A	A-VER-INFO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**		271119/331
cluster_server					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas	N/A	A-VER-CLUS-271119/332

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**		
storage_foundation_ha					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**	N/A	A-VER-STOR-271119/333
Wolfssl					
wolfssl					
Out-of-	09-11-2019	5	In wolfSSL 4.1.0 through	N/A	A-WOL-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			4.2.0c, there are missing sanity checks of memory accesses in parsing ASN.1 certificate data while handshaking. Specifically, there is a one-byte heap-based buffer overflow inside the DecodedCert structure in GetName in wolfcrypt/src/asn.c because the domain name location index is mishandled. Because a pointer is overwritten, there is an invalid free. **CVE ID : CVE-2019-18840**		WOLF-271119/334
wpwham					
currency_switcher_for_woocommerce					
Improper Input Validation	02-11-2019	4	An issue was discovered in the Currency Switcher addon before 2.11.2 for WooCommerce if a user provides a currency that was not added by the administrator. In this case, even though the currency does not exist, it will be selected, but a price amount will fall back to the default currency. This means that if an attacker provides a currency that does not exist and is worth less than this default, the attacker can eventually purchase an item for a significantly cheaper price. **CVE ID : CVE-2019-18668**	N/A	A-WPW-CURR-271119/335
Wso2					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
identity_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	4.3	WSO2 IS as Key Manager 5.7.0 allows unauthenticated reflected XSS in the dashboard user profile. **CVE ID : CVE-2019-18881**	N/A	A-WSO-IDEN-271119/336
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-11-2019	4.3	WSO2 IS as Key Manager 5.7.0 allows stored XSS in download-userinfo.jag because Content-Type is mishandled. **CVE ID : CVE-2019-18882**	N/A	A-WSO-IDEN-271119/337
xmlseclibs_project					
xmlseclibs					
Improper Input Validation	07-11-2019	6.5	Rob Richards XmlSecLibs, all versions prior to v3.0.3, as used for example by SimpleSAMLphp, performed incorrect validation of cryptographic signatures in XML messages, allowing an authenticated attacker to impersonate others or elevate privileges by creating a crafted XML message. **CVE ID : CVE-2019-3465**	N/A	A-XML-XMLS-271119/338
youphptube					
youphptube					
Improper Neutralization of Special Elements	02-11-2019	7.5	An issue was discovered in YouPHPTube through 7.7. User input passed through the live_stream_code POST	N/A	A-YOU-YOUP-271119/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			parameter to /plugin/LiveChat/getChat.json.php is not properly sanitized (in getFromChat in plugin/LiveChat/Objects/LiveChatObj.php) before being used to construct a SQL query. This can be exploited by malicious users to, e.g., read sensitive data from the database through in-band SQL Injection attacks. Successful exploitation of this vulnerability requires the Live Chat plugin to be enabled. **CVE ID : CVE-2019-18662**		
Zohocorp					
manageengine_adselfservice_plus					
Cross-Site Request Forgery (CSRF)	06-11-2019	6.8	Zoho ManageEngine ADSelfService Plus 5.x through 5803 has CSRF on the users' profile information page. Users who are attacked with this vulnerability will be forced to modify their enrolled information, such as email and mobile phone, unintentionally. Attackers could use the reset password function and control the system to send the authentication code back to the channel that the attackers own. **CVE ID : CVE-2019-18411**	N/A	A-ZOH-MANA-271119/340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operating System					
Amazon					
freertos\+fat					
Use After Free	04-11-2019	5	Real Time Engineers FreeRTOS+FAT 160919a has a use after free. The function FF_Close() is defined in ff_file.c. The file handler pxFile is freed by ffconfigFREE, which (by default) is a macro definition of vPortFree(), but it is reused to flush modified file content from the cache to disk by the function FF_FlushCache(). **CVE ID : CVE-2019-18178**	N/A	O-AMA-FREE-271119/341
ARM					
mbed-os					
Improper Input Validation	04-11-2019	5	A denial-of-service issue was discovered in the MQTT library in Arm Mbed OS 2017-11-02. The function readMQTTLenString() is called by the function MQTTDeserialize_publish() to get the length and content of the MQTT topic name. In the function readMQTTLenString(), mqttstring->lenstring.len is a part of user input, which can be manipulated. An attacker can simply change it to a larger value to invalidate the if statement so that the statements inside the if statement are skipped, letting the value of	https://github.com/ARMmbed/mbed-os/issues/11802	O-ARM-MBED-271119/342

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mqttstring->lenstring.data default to zero. Later, curn is accessed, which points to mqttstring->lenstring.data. On an Arm Cortex-M chip, the value at address 0x0 is actually the initialization value for the MSP register. It is highly dependent on the actual firmware. Therefore, the behavior of the program is unpredictable from this time on. **CVE ID : CVE-2019-17210**		
Canonical					
ubuntu_linux					
Out-of-bounds Write	13-11-2019	9.3	In generate_jsimd_ycc_rgb_convert_neon of jsimd_arm64_neon.S, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-120551338 **CVE ID : CVE-2019-2201**	N/A	O-CAN-UBUN-271119/343
Cisco					
fxos					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco	N/A	O-CIS-FXOS-271119/344

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nx-os					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance	N/A	O-CIS-NX-O-271119/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
Debian					
debian_linux					
Improper Input Validation	07-11-2019	6.5	Rob Richards XmlSecLibs, all versions prior to v3.0.3, as used for example by SimpleSAMLphp, performed incorrect validation of cryptographic signatures in XML messages, allowing an authenticated attacker to impersonate others or elevate privileges by creating a crafted XML message. **CVE ID : CVE-2019-3465**	N/A	O-DEB-DEBI-271119/346
Dell					
idrac9_firmware					
Incorrect Authorizatio	07-11-2019	4	Dell EMC iDRAC8 versions prior to 2.70.70.70 and	https://www.dell.com/	O-DEL-IDRA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			iDRAC9 versions prior to 3.36.36.36 contain an improper authorization vulnerability. A remote authenticated malicious iDRAC user with low privileges may potentially exploit this vulnerability to obtain sensitive information such as password hashes. **CVE ID : CVE-2019-3764**	support/article/sln319317/dsa-2019-137-idrac-improper-authorization-vulnerability?lang=en	271119/347
idrac8_firmware					
Incorrect Authorization	07-11-2019	4	Dell EMC iDRAC8 versions prior to 2.70.70.70 and iDRAC9 versions prior to 3.36.36.36 contain an improper authorization vulnerability. A remote authenticated malicious iDRAC user with low privileges may potentially exploit this vulnerability to obtain sensitive information such as password hashes. **CVE ID : CVE-2019-3764**	https://www.dell.com/support/article/sln319317/dsa-2019-137-idrac-improper-authorization-vulnerability?lang=en	O-DEL-IDRA-271119/348
Dlink					
dir-600_b1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1	N/A	O-DLI-DIR--271119/349

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v3.00. **CVE ID : CVE-2019-18852**		
dir-615_j1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	O-DLI-DIR--271119/350
dir-645_a1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	O-DLI-DIR--271119/351
dir-815_a1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or	N/A	O-DLI-DIR--271119/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**		
dir-823_a1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	O-DLI-DIR--271119/353
dir-842_c1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	O-DLI-DIR--271119/354

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dir-890l_a1_firmware					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	O-DLI-DIR--271119/355
fastweb					
fastgate_firmware					
Information Exposure	02-11-2019	5	Fastweb FASTGate 1.0.1b devices allow partial authentication bypass by changing a certain check_pwd return value from 0 to 1. An attack does not achieve administrative control of a device; however, the attacker can view all of the web pages of the administration console. **CVE ID : CVE-2019-18661**	N/A	O-FAS-FAST-271119/356
Fedoraproject					
fedora					
Improper Limitation of a Pathname to a Restricted Directory ('Path	06-11-2019	4.3	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10218	O-FED-FEDO-271119/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user. **CVE ID : CVE-2019-10218**		
Uncontrolled Resource Consumption	08-11-2019	5	A flaw was found in the Ceph RGW configuration with Beast as the front end handling client requests. An unauthenticated attacker could crash the Ceph RGW server by sending valid HTTP headers and terminating the connection, resulting in a remote denial of service for Ceph RGW clients. **CVE ID : CVE-2019-10222**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10222	O-FED-FEDO-271119/358
Weak Password Requirements	06-11-2019	4.9	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to verify password complexity when non-ASCII characters are used in the password, which could lead to weak	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14833	O-FED-FEDO-271119/359

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords being set for samba users, making it vulnerable to dictionary attacks. **CVE ID : CVE-2019-14833**		
NULL Pointer Dereference	06-11-2019	4	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue. **CVE ID : CVE-2019-14847**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14847	O-FED-FEDO-271119/360
Google					
android					
Improper Privilege Management	13-11-2019	10	In okToConnect of HidHostService.java, there is a possible permission bypass due to an incorrect state check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-79703832 **CVE ID : CVE-2019-2036**	N/A	O-GOO-ANDR-271119/361
Improper Input Validation	13-11-2019	7.2	In call of SliceProvider.java, there is a possible permissions bypass due to improper input validation. This could lead to local escalation of privilege with	N/A	O-GOO-ANDR-271119/362

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-138441555 **CVE ID : CVE-2019-2192**		
Improper Privilege Managemen t	13-11-2019	7.2	In WelcomeActivity.java and related files, there is a possible permissions bypass due to a partially provisioned Device Policy Client. This could lead to local escalation of privilege, leaving an Admin app installed with no indication to the user, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-132261064 **CVE ID : CVE-2019-2193**	N/A	O-GOO-ANDR-271119/363
Improper Input Validation	13-11-2019	7.2	In tokenize of sqlite3_android.cpp, there is a possible attacker controlled INSERT statement due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9	N/A	O-GOO-ANDR-271119/364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android-10Android ID: A-139186193 **CVE ID : CVE-2019-2195**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-11-2019	4.9	In Download Provider, there is possible SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-135269143 **CVE ID : CVE-2019-2196**	N/A	O-GOO-ANDR-271119/365
N/A	13-11-2019	2.1	In processPhonebookAccess of CachedBluetoothDevice.java, there is a possible permission bypass due to an insecure default value. This could lead to local information disclosure of the user's contact list with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-138529441 **CVE ID : CVE-2019-2197**	N/A	O-GOO-ANDR-271119/366
Improper Neutralization of Special Elements used in an	13-11-2019	4.9	In Download Provider, there is a possible SQL injection vulnerability. This could lead to local information disclosure with no additional	N/A	O-GOO-ANDR-271119/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-135270103 **CVE ID : CVE-2019-2198**		
Improper Privilege Managemen t	13-11-2019	7.2	In createSessionInternal of PackageInstallerService.java, there is a possible permissions bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-138650665 **CVE ID : CVE-2019-2199**	N/A	O-GOO-ANDR-271119/368
Out-of-bounds Write	13-11-2019	9.3	In generate_jsimd_ycc_rgb_con vert_neon of jsimd_arm64_neon.S, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-120551338	N/A	O-GOO-ANDR-271119/369

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2201		
Out-of-bounds Write	13-11-2019	7.2	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-137283376 **CVE ID : CVE-2019-2202**	N/A	O-GOO-ANDR-271119/370
Out-of-bounds Write	13-11-2019	7.2	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-137370777 **CVE ID : CVE-2019-2203**	N/A	O-GOO-ANDR-271119/371
Out-of-bounds Read	13-11-2019	10	In FindSharedFunctionInfo of objects.cc, there is a possible out of bounds read due to a mistake in AST traversal. This could lead to remote code execution in the pacprocessor with no additional execution privileges needed. User interaction is not needed for	N/A	O-GOO-ANDR-271119/372

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-9Android ID: A-138442295 **CVE ID : CVE-2019-2204**		
Use After Free	13-11-2019	10	In ProxyResolverV8::SetPacScript of proxy_resolver_v8.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-139806216 **CVE ID : CVE-2019-2205**	N/A	O-GOO-ANDR-271119/373
Out-of-bounds Write	13-11-2019	9.3	In rw_i93_sm_set_read_only of rw_i93.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-139188579 **CVE ID : CVE-2019-2206**	N/A	O-GOO-ANDR-271119/374
Out-of-bounds Write	13-11-2019	7.2	In nfa_hci_handle_admin_gate_rsp of nfa_hci_act.cc, there is a possible out of bound write	N/A	O-GOO-ANDR-271119/375

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to missing bounds checks. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-124524315 **CVE ID : CVE-2019-2207**		
Information Exposure	13-11-2019	7.8	There is a possible out of bounds read in v8 JIT code due to a bug in code generation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-138441919 **CVE ID : CVE-2019-2208**	N/A	O-GOO-ANDR-271119/376
Out-of-bounds Read	13-11-2019	4.9	In BTA_DmPinReply of bta_dm_api.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-139287605	N/A	O-GOO-ANDR-271119/377

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-2209		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-11-2019	7.2	In load_logging_config of qmi_vs_service.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-139148442 **CVE ID : CVE-2019-2210**	N/A	O-GOO-ANDR-271119/378
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-11-2019	7.8	In createProjectionMapForQuery of TvProvider.java, there is possible SQL injection. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-135269669 **CVE ID : CVE-2019-2211**	N/A	O-GOO-ANDR-271119/379
Information Exposure	13-11-2019	4.9	In poisson_distribution of random, there is an out of bounds read. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-	N/A	O-GOO-ANDR-271119/380

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0 Android-8.1 Android-9 Android-10Android ID: A-139690488 **CVE ID : CVE-2019-2212**		
Use After Free	13-11-2019	6.9	In binder_free_transaction of binder.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-133758011References: Upstream kernel **CVE ID : CVE-2019-2213**	N/A	O-GOO-ANDR-271119/381
Improper Privilege Managemen t	13-11-2019	7.2	In binder_transaction of binder.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-136210786References: Upstream kernel **CVE ID : CVE-2019-2214**	N/A	O-GOO-ANDR-271119/382
Improper Privilege Managemen t	13-11-2019	7.2	In getUserCount and getCount of UserSwitcherController.java, there is possible new user creation due to a logic error. This could lead to local	N/A	O-GOO-ANDR-271119/383

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140486529 **CVE ID : CVE-2019-2233**		
Improper Input Validation	13-11-2019	7.5	In the Broadcom Wi-Fi driver, there is a possible out of bounds write due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-130375182 **CVE ID : CVE-2019-9466**	N/A	O-GOO-ANDR-271119/384
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	13-11-2019	7.2	In the Bootloader, there is a possible kernel command injection due to missing command sanitization. This could lead to a local elevation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-80316910 **CVE ID : CVE-2019-9467**	N/A	O-GOO-ANDR-271119/385
HP					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
prodesk_490_g2_mt_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/386
prodesk_490_g3_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/387

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-16284		
prodesk_498_g2_mt_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/388
prodesk_498_g3_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
prodesk_600_g2_dm_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/390
prodesk_600_g2_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
proone_400_g2_aio_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROO-271119/392
proone_600_g2_aio_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	O-HP-PROO-271119/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
rp2_retail_system_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-RP2_-271119/394
rp9_g1_retail_system_9015_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	O-HP-RP9_-271119/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
rp9_g1_retail_system_9018_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-RP9_-271119/396
zbook_14_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_14_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/398
zbook_15_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_15_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/400
zbook_15_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_15u_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/402
zbook_15u_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_17_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/404
zbook_17_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_17_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/406
zbook_studio_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The	https://support.hp.com/rs-en/document/c06456250	O-HP-ZBOO-271119/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
z1_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-Z1_G-271119/408
z2_mini_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in	https://support.hp.com/rs-en/document/c06456250	O-HP-Z2_M-271119/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
z238_microtower_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-Z238-271119/410
z240_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot	https://support.hp.com/rs-en/document/c06456250	O-HP-Z240-271119/411

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
z240_tower_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-Z240-271119/412
sprout_pro_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution	https://support.hp.com/rs-en/document/c064562	O-HP-SPRO-271119/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	50	
pro_x2_612_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PRO_-271119/414
probook_11_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which	https://support.hp.com/rs-en/docume	O-HP-PROB-271119/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	nt/c06456250	
probook_11_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/416
probook_430_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP	https://support.hp.com/rs-	O-HP-PROB-271119/417

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	en/document/c06456250	
probook_430_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/418
probook_430_g3_firmware					
Improper Input	05-11-2019	9	A potential security vulnerability has been	https://support.hp.com	O-HP-PROB-271119/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	/rs-en/document/c06456250	
probook_440_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/420
probook_440_g2_firmware					
Improper	05-11-2019	9	A potential security	https://sup	O-HP-PROB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	port.hp.com/rs-en/document/c06456250	271119/421
probook_440_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/422
probook_450_g1_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/423
probook_450_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/424

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
probook_450_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/425
probook_470_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/426

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16284		
probook_470_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/427
probook_470_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/428

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_640_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/429
probook_640_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/430

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_650_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/431
probook_650_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_x360_11_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROB-271119/433
prodesk_400_g1_dm_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
prodesk_400_g2_dm_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/435
prodesk_400_g2.5_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/436

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
prodesk_400_g3_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/437
prodesk_405_g2_mt_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
prodesk_485_g2_mt_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/439
prodesk_480_g3_sff_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	O-HP-PROD-271119/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_820_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/441
elitebook_820_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_820_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/443
elitebook_828_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/444

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_840_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/445
elitebook_840_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_840_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/447
elitebook_848_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_850_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/449
elitebook_850_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_850_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/451
elitebook_folio_1020_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution	https://support.hp.com/rs-en/document/c064562	O-HP-ELIT-271119/452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	50	
elitebook_folio_1040_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/453
elitebook_folio_1040_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which	https://support.hp.com/rs-en/docume	O-HP-ELIT-271119/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	nt/c06456250	
elitebook_folio_9480m_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/455
elitebook_folio_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP	https://support.hp.com/rs-	O-HP-ELIT-271119/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	en/document/c06456250	
elitebook_revolve_810_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/457
elitebook_revolve_810_g3_firmware					
Improper Input	05-11-2019	9	A potential security vulnerability has been	https://support.hp.com	O-HP-ELIT-271119/458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	/rs-en/document/c06456250	
elitedesk_800_g2_dm_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/459
elitedesk_800_g2_sff_firmware					
Improper	05-11-2019	9	A potential security	https://sup	O-HP-ELIT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	port.hp.com/rs-en/document/c06456250	271119/460
elitedesk_800_g2_twr_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/461
eliteone_800_g2_aio_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/462
elitepad_1000_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/463

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mp9_g2_retail_system_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-MP9_-271119/464
pro_tablet_10_ee_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	O-HP-PRO_-271119/465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16284		
pro_tablet_608_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-PRO_-271119/466
pro_tablet_610_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	O-HP-PRO_-271119/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
d3q21a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/468
d3q21b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/469
d3q21c_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/470
d3q21d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert.	N/A	O-HP-D3Q2-271119/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
k9z76a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-K9Z7-271119/472
k9z76b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-K9Z7-271119/473
k9z76d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-K9Z7-271119/474
260_g1_dm_firmware					
Improper	05-11-2019	9	A potential security	https://sup	O-HP-260_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	port.hp.com/rs-en/document/c06456250	271119/475
280_pro_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-280_-271119/476
285_g2_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-285_-271119/477
340_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-340_-271119/478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
340_g4_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-340_-271119/479
346_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	O-HP-346_-271119/480

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16284		
346_g4_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-346_-271119/481
348_g3_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	O-HP-348_-271119/482

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
348_g4_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-348_-271119/483
elite_slice_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elite_x2_1011_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/485
elite_x2_1012_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_1030_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/487
elitebook_1040_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_720_g1__firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/489
elitebook_720_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_740_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/491
elitebook_740_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_750_g1_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/493
elitebook_750_g2_firmware					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	O-HP-ELIT-271119/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
d9l63a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D9L6-271119/495
d9l64a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D9L6-271119/496
t0g70a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-T0G7-271119/497

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
j3p65a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J3P6-271119/498
j3p68a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J3P6-271119/499
j6u57a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J6U5-271119/500
j6u57b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a	N/A	O-HP-J6U5-271119/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local device. **CVE ID : CVE-2019-6337**		
j9v80a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J9V8-271119/502
j9v80b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J9V8-271119/503
j6u55a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J6U5-271119/504
j6u55d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert.	N/A	O-HP-J6U5-271119/505

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
j6u51b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J6U5-271119/506
j9v82a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J9V8-271119/507
j9v82d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-J9V8-271119/508
j9v78b_firmware					
Reachable	07-11-2019	3.3	For the printers listed a	N/A	O-HP-J9V7-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		271119/509
d3q15a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/510
d3q15b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/511
d3q15d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d3q16a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/513
d3q16d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/514
w2z52b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-W2Z5-271119/515
d3q19a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a	N/A	O-HP-D3Q1-271119/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local device. **CVE ID : CVE-2019-6337**		
d3q19b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/517
d3q19d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/518
d3q20a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/519
d3q20b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert.	N/A	O-HP-D3Q2-271119/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
d3q20c_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/521
d3q20d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q2-271119/522
w2z53b_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-W2Z5-271119/523
2dr21d_firmware					
Reachable	07-11-2019	3.3	For the printers listed a	N/A	O-HP-2DR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		271119/524
d3q17a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/525
d3q17d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-D3Q1-271119/526
k9z74a_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-K9Z7-271119/527

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
k9z74d_firmware					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	O-HP-K9Z7-271119/528
hpe					
nimbleos					
Improper Privilege Management	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	O-HPE-NIMB-271119/529
Huawei					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
honor_v20_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20 smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system does not lock certain function properly, when the function is called by multiple processes could cause out of bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**	N/A	O-HUA-HONO-271119/530
ar1200-s_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR12-271119/531
Out-of-	13-11-2019	5	There is an out of bound	N/A	O-HUA-AR12-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		271119/532
ar1200_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR12-271119/533
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR12-271119/534
ar150_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR15-271119/535
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR15-271119/536
ar160_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR16-271119/537
Out-of-	13-11-2019	5	There is an out of bound	N/A	O-HUA-AR16-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		271119/538
ar2200_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR22-271119/539
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR22-271119/540
ar3200_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR32-271119/541
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR32-271119/542
srg1300_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-SRG1-271119/543
Out-of-	13-11-2019	5	There is an out of bound	N/A	O-HUA-SRG1-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		271119/544
srg2300_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-SRG2-271119/545
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-SRG2-271119/546
srg3300_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-SRG3-271119/547
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-SRG3-271119/548
p20_pro_firmware					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of	N/A	O-HUA-P20_-271119/549

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**		
mate_rs_firmware					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**	N/A	O-HUA-MATE-271119/550
taurus-al00b_firmware					
Improper Authentication	13-11-2019	6.8	Huawei smartphones with versions earlier than Taurus-AL00B	N/A	O-HUA-TAUR-271119/551

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.41(SP2C00E41R3P2) have an improper authentication vulnerability. Successful exploitation may cause the attacker to access specific components. **CVE ID : CVE-2019-5233**		
elle-al00b_firmware					
Insufficient Verification of Data Authenticity	13-11-2019	4.6	Smartphones with software of ELLE-AL00B 9.1.0.109(C00E106R1P21), 9.1.0.113(C00E110R1P21), 9.1.0.125(C00E120R1P21), 9.1.0.135(C00E130R1P21), 9.1.0.153(C00E150R1P21), 9.1.0.155(C00E150R1P21), 9.1.0.162(C00E160R2P1) have an insufficient verification vulnerability. The system does not verify certain parameters sufficiently, an attacker should connect to the phone and gain high privilege to launch the attack. Successful exploit could cause DOS or malicious code execution. **CVE ID : CVE-2019-5246**	N/A	O-HUA-ELLE-271119/552
emily-al00a_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C	N/A	O-HUA-EMIL-271119/553

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
emily-tl00b_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same	N/A	O-HUA-EMIL-271119/554

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
emily-l09c_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**	N/A	O-HUA-EMIL-271119/555
hima-l09ca_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21),	N/A	O-HUA-HIMA-271119/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
hima-l29ca_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12)	N/A	O-HUA-HIMA-271119/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
hima-l29c_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**	N/A	O-HUA-HIMA-271119/558
honor_10_lite_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before 9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**	N/A	O-HUA-HONO-271119/559
honor_8a_firmware					
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before 9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**	N/A	O-HUA-HONO-271119/560
huawei_y6_firmware					
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before	N/A	O-HUA-HUAW-271119/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**		
ar120-s_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR12-271119/562
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal.	N/A	O-HUA-AR12-271119/563

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5294		
p30_pro_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20 smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system does not lock certain function properly, when the function is called by multiple processes could cause out of bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**	N/A	O-HUA-P30_-271119/564
p30_firmware					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20 smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system	N/A	O-HUA-P30_-271119/565

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not lock certain function properly, when the function is called by multiple processes could cause out of bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**		
Insufficient Verification of Data Authenticity	12-11-2019	4.6	P30 smartphones with versions earlier than ELLE-AL00B 9.1.0.193(C00E190R2P1) have an insufficient verification vulnerability. The system does not verify certain parameters sufficiently, an attacker should connect to the phone and gain high privilege to launch the attack, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5229**	N/A	O-HUA-P30_-271119/566
Incorrect Authorization	13-11-2019	2.1	P30 smartphones with versions earlier than ELLE-AL00B 9.1.0.186(C00E180R2P1) have an improper authorization vulnerability. The software incorrectly performs an authorization check when a user attempts to perform certain action. Successful exploit could allow the attacker to update a crafted package.	N/A	O-HUA-P30_-271119/567

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5231		
honor_play_firmware					
Improper Authentication	12-11-2019	1.9	Honor play smartphones with versions earlier than Cornell-AL00A 9.1.0.321(C00E320R1P1T8) have an insufficient authentication vulnerability. The system has a logic judge error under certain scenario. Successful exploit could allow the attacker to modify the alarm clock settings after a serious of uncommon operations without unlock the screen lock. **CVE ID : CVE-2019-5213**	N/A	O-HUA-HONO-271119/568
emily-l29c_firmware					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same	N/A	O-HUA-EMIL-271119/569

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
p20_firmware					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**	N/A	O-HUA-P20_-271119/570
ar150-s_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages	N/A	O-HUA-AR15-271119/571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**		
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR15-271119/572
ar200					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR20-271119/573
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message,	N/A	O-HUA-AR20-271119/574

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		
ar200-s_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR20-271119/575
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR20-271119/576
ar2200-s_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages	N/A	O-HUA-AR22-271119/577

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**		
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-AR22-271119/578
ar3600_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-AR36-271119/579
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message,	N/A	O-HUA-AR36-271119/580

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		
netengine16ex_firmware					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	O-HUA-NETE-271119/581
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	O-HUA-NETE-271119/582
IBM					
i					
Improper Neutralization of Input During Web Page Generation	09-11-2019	4.3	IBM i 7.2, 7.3, and 7.4 for i is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	https://www.ibm.com/support/pages/node/1100085	O-IBM-I-271119/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163492. **CVE ID : CVE-2019-4450**		
intelbras					
wrn_150_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-11-2019	4.3	An issue was discovered on Intelbras WRN 150 1.0.17 devices. There is stored XSS in the Service Name tab of the WAN configuration screen, leading to a denial of service (inability to change the configuration). **CVE ID : CVE-2019-17222**	N/A	O-INT-WRN_-271119/584
Lenovo					
legion_c530-19icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/585
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/586
legion_c730-19ico_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-LEGI-271119/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/588
legion_t530-28icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/589
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/590
legion_t730-28ico_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/591
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/592

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkcentre_m610_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/593
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/594
thinkcentre_m6500t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/595
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/596
thinkcentre_m6500s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/597
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/598
thinkcentre_m6600_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/599
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/600
thinkcentre_m6600q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/601
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/602
thinkcentre_m6600t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/603

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/604
thinkcentre_m6600s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/605
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/606
thinkcentre_m700q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/607
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/608

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
thinkcentre_m710q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/609
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/610
thinkcentre_m720q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/611
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/612
thinkcentre_m720s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/613

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/614
thinkcentre_m73p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/615
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/616
thinkcentre_m800_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/617
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/618
thinkcentre_m8500t_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/620
thinkcentre_m8500s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/621
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/622
thinkcentre_m8600t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/623
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m8600s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/625
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/626
thinkcentre_m900_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/627
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/628
thinkcentre_m910t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/629

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/630
thinkcentre_m910s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/631
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/632
thinkcentre_m910q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/633
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/634
thinkcentre_m910x_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/635
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/636
thinkcentre_m920q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/637
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/638
thinkcentre_m920x_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/639
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
yangtian_afh110_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/641
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/642
yangtian_afh81_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/643
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/644
yangtian_mc_h110_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-YANG-271119/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/646
yangtian_mc_h110_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/647
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/648
yangtian_mc_h81_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/649
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/650

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
yangtian_ytm6900e-00_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/651
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/652
zhaoyang_e53-80_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-ZHAO-271119/653
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-ZHAO-271119/654
xiaoxin_air-15iwl_2019_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/655
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-XIAO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/656
xiaoxin-14_2019iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/657
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/658
xiaoxin-14iwl_qc_2019_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/659
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/660
xiaoxin-15_2019iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-XIAO-271119/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/662
xx_chao5000-ikbra_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XX_C-271119/663
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XX_C-271119/664
y7000_2019_1050_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-Y700-271119/665
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-Y700-271119/666

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
yoga_520-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/667
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/668
yoga_730-13iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/669
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/670
yoga_730-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/671

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/672
yoga_s730-13iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/673
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/674
yoga_s940-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/675
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/676
yoga530-14ikb_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-YOGA-271119/677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/678
flex_6-1470_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-FLEX-271119/679
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-FLEX-271119/680
zhaoyang_k42-80_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-ZHAO-271119/681
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-ZHAO-271119/682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
xiaoxin_tide_7000-15_u22_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/683
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/684
xiaoxin_tide_7000-15_u42_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/685
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/686
zhaoyang_e43-80_kbl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-ZHAO-271119/687

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-ZHAO-271119/688
l340-15irh_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-L340-271119/689
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-L340-271119/690
l340-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-L340-271119/691
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-L340-271119/692
l340-17irh_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-L340-271119/693
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-L340-271119/694
l340-15iwltouch_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-L340-271119/695
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-L340-271119/696
l340-17iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-L340-271119/697
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-L340-271119/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
legion_y530-15ich_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/699
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/700
legion_y730-15ich_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/701
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/702
legion_y7000p-1060_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-LEGI-271119/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/704
legion_y530-15ich\(1060\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/705
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/706
legion_y730-17ich_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/707
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/708

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_y740-15irhg_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/709
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/710
legion_y740-15ichg_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/711
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/712
legion_y9000k_2019_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/713
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-LEGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/714
legion_y740-17ichg_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/715
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/716
legion_y740-17irhg_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/717
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/718
legion_y9000p_2019_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-LEGI-271119/719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/720
lenovo_v720-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LENO-271119/721
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LENO-271119/722
v410z\(yt_s4250\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V410-271119/723
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-V410-271119/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
330-14ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/725
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/726
330-15ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/727
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/728
330-15ikbr_touch_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/729

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/730
330-17ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/731
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/732
720s_touch-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-720S-271119/733
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-720S-271119/734
720s-15ikb_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-720S-271119/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-720S-271119/736
flex_5-1570\(r\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-FLEX-271119/737
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-FLEX-271119/738
k43c-80_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-K43C-271119/739
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-K43C-271119/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
v330-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V330-271119/741
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V330-271119/742
v330-14isk_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V330-271119/743
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V330-271119/744
v330-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-V330-271119/745

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V330-271119/746
v330-15isk_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V330-271119/747
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V330-271119/748
v730-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V730-271119/749
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V730-271119/750
yoga_730-13ikb_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/751
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/752
yoga_730-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/753
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/754
thinkpad_11e_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/755
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
miix_720-12ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-MIIX-271119/757
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-MIIX-271119/758
rescuer_y7000p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-RESC-271119/759
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-RESC-271119/760
rescuer_y7000p\(1060\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-RESC-271119/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-RESC-271119/762
rescuer_y7000_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-RESC-271119/763
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-RESC-271119/764
rescuer_y7000\(1060\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-RESC-271119/765
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-RESC-271119/766

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
s145-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S145-271119/767
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S145-271119/768
s145-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S145-271119/769
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S145-271119/770
s145-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S145-271119/771
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-S145-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/772
s145-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S145-271119/773
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S145-271119/774
340c-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-340C-271119/775
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-340C-271119/776
s340-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-S340-271119/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S340-271119/778
thinkstation_p310_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/779
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/780
thinkcentre_x1_aio_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/781
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
s340-14iwl_touch_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S340-271119/783
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S340-271119/784
s340-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S340-271119/785
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S340-271119/786
s340-15iwl_touch_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S340-271119/787

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S340-271119/788
s530-13iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S530-271119/789
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S530-271119/790
s540-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S540-271119/791
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S540-271119/792
s540-14iwl_touch_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-S540-271119/793

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S540-271119/794
s540-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S540-271119/795
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-S540-271119/796
s940-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-S940-271119/797
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-S940-271119/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
v110-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V110-271119/799
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V110-271119/800
v110-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V110-271119/801
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V110-271119/802
v130-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-V130-271119/803

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V130-271119/804
v130-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V130-271119/805
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V130-271119/806
v310-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V310-271119/807
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V310-271119/808
v310-14isk_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V310-271119/809
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V310-271119/810
v310-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V310-271119/811
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V310-271119/812
v310-15isk_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V310-271119/813
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-V310-271119/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
v320-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V320-271119/815
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V320-271119/816
v320-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V320-271119/817
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V320-271119/818
v320-17ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-V320-271119/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V320-271119/820
v510-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V510-271119/821
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V510-271119/822
v510-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V510-271119/823
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V510-271119/824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wei5-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-WEI5-271119/825
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-WEI5-271119/826
wei5-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-WEI5-271119/827
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-WEI5-271119/828
xiaoxin_air_13iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/829
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-XIAO-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/830
xiaoxin_air_14ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/831
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/832
xiaoxin_air_14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/833
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/834
xiaoxin_air_15ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-XIAO-271119/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/836
xiaoxin_air_15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/837
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-XIAO-271119/838
xiaoxin_air-14iwl_2019_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-XIAO-271119/839
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-XIAO-271119/840

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
thinkpad_10_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/841
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/842
yoga_11e_3rd_gen_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/843
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/844
yoga_11e_4th_gen_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGA-271119/845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGA-271119/846
thinkpad_e450_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/847
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/848
thinkpad_e450c_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/849
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/850
thinkpad_e550_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/852
thinkpad_e550c_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/853
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/854
thinkpad_e490s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/855
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_s3_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/857
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/858
510-15ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-510--271119/859
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-510--271119/860
510s-08ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-510S-271119/861

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-510S-271119/862
aio520-22ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/863
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO5-271119/864
aio520-22iku_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/865
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO5-271119/866
aio520-24ikl_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/867
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO5-271119/868
aio520-24iku_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/869
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO5-271119/870
aio520-27ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/871
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-AIO5-271119/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
h50-30g_desktop_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-H50--271119/873
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-H50--271119/874
ideacentre_300-20ish_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/875
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/876
ideacentre_300s-11ish_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-IDEA-271119/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/878
ideacentre_510s-08ish_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/879
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/880
legion_y520t_z370_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/881
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/882

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
m4500_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-M450-271119/883
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-M450-271119/884
m4500_id_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-M450-271119/885
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-M450-271119/886
m4550_id_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-M455-271119/887
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-M455-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/888
qitian_4500_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QITI-271119/889
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/890
qitian_b4550_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QITI-271119/891
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/892
qitian_b4650_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-QITI-271119/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/894
qitian_m4550_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QITI-271119/895
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/896
qitian_m4600_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QITI-271119/897
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-QITI-271119/898

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
qitian_m4650_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QITI-271119/899
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/900
qt_a7400_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QT_A-271119/901
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QT_A-271119/902
qt_b415_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QT_B-271119/903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QT_B-271119/904
qt_m410_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QT_M-271119/905
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QT_M-271119/906
qt_m415_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-QT_M-271119/907
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QT_M-271119/908
thinkcentre_e73s_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/910
thinkcentre_e74_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/911
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/912
thinkcentre_e74s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/913
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_e74z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/915
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/916
thinkcentre_e75s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/917
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/918
thinkcentre_e75t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/920
thinkcentre_m4500k_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/921
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/922
thinkcentre_m4500q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/923
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/924
thinkcentre_m4500s_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/925
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/926
thinkcentre_m4500t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/927
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/928
thinkcentre_m4600s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/929
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m4600t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/931
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/932
thinkcentre_m700s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/933
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/934
thinkcentre_m700t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-THIN-271119/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/936
thinkcentre_m700z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/937
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/938
thinkcentre_m710e_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/939
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/940

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkcentre_m710s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/941
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/942
thinkcentre_m710t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/943
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/944
thinkcentre_m720t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/945
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/946
thinkcentre_m7300z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/947
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/948
thinkcentre_m73_tiny_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/949
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/950
thinkcentre_m800z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/951

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/952
thinkcentre_m810z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/953
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/954
thinkcentre_m818z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/955
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/956

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
thinkcentre_m820z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/957
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/958
thinkcentre_m8300z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/959
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/960
thinkcentre_m8350z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/961

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/962
thinkcentre_m900z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/963
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/964
thinkcentre_m910z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/965
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/966
thinkcentre_m920z_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/967

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/968
thinkcentre_m9500z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/969
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/970
thinkcentre_m9550z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/971
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_s510_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/973
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/974
v520s-08ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V520-271119/975
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V520-271119/976
v520t-15ikl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-V520-271119/977

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V520-271119/978
thinkcentre_m920t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/979
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/980
thinkpad_13_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/981
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/982
thinkcentre_m920s_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/983
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/984
thinkcentre_m93_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/985
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/986
thinkpad_e460_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/987
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_e560_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/989
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/990
thinkpad_e470_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/991
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/992
yangtian_afq150_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-YANG-271119/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/994
thinkpad_e570_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/995
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/996
thinkpad_e480_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/997
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/998

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e580_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/999
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1000
thinkpad_s5_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1001
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1002
thinkpad_l380_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1003
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1004
yta8900f_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YTA8-271119/1005
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YTA8-271119/1006
thinkpad_l380_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1007
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1008
thinkpad_l460_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/1009

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1010
thinkpad_l470_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1011
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1012
thinkpad_l480_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1013
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/1014

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
ideacentre_730s-24ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1015
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1016
thinkpad_l580_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1017
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1018
thinkpad_l560_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1020
thinkpad_l570_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1021
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1022
thinkcentre_e95z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1023
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1024
thinkcentre_e96z_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1026
thinkpad_p50_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1027
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1028
thinkpad_p50s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1029
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/1030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_p51s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1031
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1032
thinkcentre_m83z_\(aio\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1033
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1034
qitian_a815_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-QITI-271119/1035

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/1036
thinkcentre_m9350z_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1037
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1038
thinkcentre_m93z_\(aio\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1039
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1040
v540-24iwl\(yt_s5430\)_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V540-271119/1041
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V540-271119/1042
yogo_a940-27icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YOGO-271119/1043
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YOGO-271119/1044
130-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-130--271119/1045
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-130--271119/1046

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
130-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-130--271119/1047
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-130--271119/1048
330-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/1049
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/1050
330-15ich_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-330--271119/1051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/1052
330-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/1053
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/1054
330-17ich_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/1055
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/1056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
330-17ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330--271119/1057
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330--271119/1058
330c-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330C-271119/1059
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330C-271119/1060
330c-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330C-271119/1061
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-330C-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1062
330c-15ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-330C-271119/1063
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-330C-271119/1064
340c-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-340C-271119/1065
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-340C-271119/1066
530s-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-530S-271119/1067

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-530S-271119/1068
530s-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-530S-271119/1069
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-530S-271119/1070
530s-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-530S-271119/1071
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-530S-271119/1072

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
530s-15ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-530S-271119/1073
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-530S-271119/1074
720s-14ikbr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-720S-271119/1075
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-720S-271119/1076
730s-13iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-730S-271119/1077

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-730S-271119/1078
c340-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-C340-271119/1079
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-C340-271119/1080
c340-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-C340-271119/1081
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-C340-271119/1082
e42-80_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-E42--271119/1083

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-E42--271119/1084
e52-80_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-E52--271119/1085
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-E52--271119/1086
flex_6-14ikb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-FLEX-271119/1087
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-FLEX-271119/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
flex-14iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-FLEX-271119/1089
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-FLEX-271119/1090
flex-15iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-FLEX-271119/1091
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-FLEX-271119/1092
thinkpad_p52s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/1093

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1094
thinkpad_p70_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1095
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1096
thinkpad_e560p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1097
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1098
thinkpad_t25_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1099
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1100
thinkpad_t460_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1101
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1102
thinkpad_t460p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1103
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/1104

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_t460s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1105
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1106
thinkpad_t470_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1107
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1108
thinkpad_t470p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-THIN-271119/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1110
thinkpad_t470s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1111
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1112
thinkpad_t480_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1113
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1114

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t480s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1115
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1116
thinkpad_t560_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1117
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1118
thinkpad_t570_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1119
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1120
thinkpad_t580_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1121
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1122
thinkpad_x1_carbon_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1123
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1124
thinkpad_x1_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/1125

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1126
thinkpad_x1_tablet_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1127
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1128
thinkpad_x260_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1129
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/1130

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
thinkpad_x270_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1131
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1132
thinkpad_x280_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1133
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1134
thinkpad_x380_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1135

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1136
thinkpad_yoga_370_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1137
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1138
v310z\(yt_s3150\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V310-271119/1139
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V310-271119/1140
v510z_\(yt_s5250\)_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-V510-271119/1141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V510-271119/1142
v530-22icb\(yt_s4350\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V530-271119/1143
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V530-271119/1144
v530-24icb\(yt_s5350\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V530-271119/1145
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-V530-271119/1146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkstation_e32_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1147
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1148
thinkstation_p300_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1149
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1150
thinkstation_p318_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/1151

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1152
thinkstation_p320_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1153
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1154
thinkstation_p320_tiny_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1155
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1156
thinkstation_p330_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1157
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1158
thinkstation_p330_tiny_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1159
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1160
ideacentre_510-15icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1161
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-IDEA-271119/1162

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
ideacentre_510a-15icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1163
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1164
ideacentre_700_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1165
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1166
ideacentre_720-18icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-IDEA-271119/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1168
thinkpad_t440p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1169
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1170
thinkpad_t450_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1171
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t450s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1173
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1174
thinkpad_t490_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1175
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1176
thinkpad_t490s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1177
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1178
thinkpad_t540p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1179
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1180
thinkpad_t550_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1181
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1182
thinkpad_t590_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1184
thinkpad_tablet_10_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1185
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1186
thinkpad_tablet_8_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1187
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/1188

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkpad_w540_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1189
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1190
thinkpad_w541_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1191
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1192
thinkpad_w550s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1193

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1194
thinkpad_x1_extreme_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1195
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1196
thinkpad_x131e_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1197
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1198
thinkpad_x140e_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1200
thinkpad_x240_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1201
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1202
thinkpad_x240s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1203
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_x250_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1205
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1206
thinkpad_x390_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1207
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1208
thinkpad_x390_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/1209

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1210
thinkpad_yoga_11e_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1211
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1212
thinkpad_yoga_260-s1_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1213
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1214
thinksystem_hr630x_\(skl\)_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1215
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1216
thinksystem_hr650x_\(skl\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1217
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1218
thinksystem_odc5200-cn650s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1219
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/1220

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_s1_3rd_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1221
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1222
ideacentre_310s-08asr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1223
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1224
ideacentre_310s-08igm_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-IDEA-271119/1225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1226
ideacentre_720-18apr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-IDEA-271119/1227
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-IDEA-271119/1228
legion_t530-28apr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/1229
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/1230

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_t530-28apr_reflash_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/1231
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/1232
legion_t530-28icb_reflash_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-LEGI-271119/1233
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-LEGI-271119/1234
63_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-63_F-271119/1235
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-63_F-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1236
v330-15igm_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V330-271119/1237
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V330-271119/1238
v530s-07icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-V530-271119/1239
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-V530-271119/1240
qitian_b5900_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-QITI-271119/1241

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-QITI-271119/1242
thinkcentre_e73_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1243
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1244
thinkcentre_e93_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1245
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/1246

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkcentre_m600_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1247
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1248
thinkcentre_m625q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1249
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1250
thinkcentre_m715q_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1251

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1252
thinkcentre_m715q_rr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1253
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1254
thinkcentre_m715t_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1255
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1256
thinkpad_e490_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1258
thinkpad_e590_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1259
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1260
thinkpad_r490_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1261
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/1262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_r590_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1263
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1264
thinkpad_helix_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1265
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1266
thinkpad_s3_3rd_gen_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/1267

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1268
thinkpad_s2_yoga_3rd_gen_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1269
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1270
thinkpad_l390_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1271
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1272
thinkpad_s2_yoga_4th_gen_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1273
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1274
thinkpad_l450_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1275
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1276
thinkpad_l490_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1277
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-THIN-271119/1278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_l590_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1279
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1280
thinkpad_p1_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1281
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1282
thinkpad_p43s_\(20rx\)_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-THIN-271119/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1284
thinkpad_p51_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1285
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1286
thinkpad_p52_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1287
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1288

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_p53_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1289
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1290
thinkpad_p53s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1291
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1292
thinkpad_p71_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1293
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-THIN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1294
thinkpad_p72_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1295
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1296
thinkpad_p73_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1297
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1298
thinkpad_s1_yoga_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-THIN-271119/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1300
thinkpad_s5_2nd_generation_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1301
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1302
thinkpad_s5_yoga_15_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1303
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-THIN-271119/1304

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
thinkpad_s531_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1305
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1306
thinkpad_s540_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1307
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1308
thinkpad_t440_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1310
thinkpad_t440s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1311
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1312
thinkcentre_m715s_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1313
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1314
thinkcentre_m725s_firmware					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	O-LEN-THIN-271119/1315

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1316
thinkcentre_m73_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1317
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1318
thinkcentre_m79_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1319
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	O-LEN-THIN-271119/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m83_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1321
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1322
thinkcentre_m90n-1_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-THIN-271119/1323
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1324
thinkcentre_m93p_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	O-LEN-THIN-271119/1325

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-THIN-271119/1326
yangtian_me_h110_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1327
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1328
yangtian_we_h110_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1329
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1330
yangtian_mf_h110_pci_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1331
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1332
yangtian_wf_h110_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1333
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1334
yangtian_mf_h81_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1335
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	O-LEN-YANG-271119/1336

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
yangtian_wf_h81_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1337
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1338
yangtian_ms_h81_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1339
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1340
yangtian_ws_h81_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	O-LEN-YANG-271119/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1342
yangtian_tc_h110_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1343
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1344
yangtian_wc_h110_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1345
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1346

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
yangtian_tc_h81_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1347
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1348
yangtian_wcc_h81_pci_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-YANG-271119/1349
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-YANG-271119/1350
a340-22_iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-A340-271119/1351
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	O-LEN-A340-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/1352
a340-24_iwl_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-A340-271119/1353
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-A340-271119/1354
a340-22icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-A340-271119/1355
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-A340-271119/1356
a340-24icb_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	O-LEN-A340-271119/1357

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-A340-271119/1358
a340-22ast_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-A340-271119/1359
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-A340-271119/1360
aio_330-20ast_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO_-271119/1361
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	O-LEN-AIO_-271119/1362

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
aio_330-20igm_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO_-271119/1363
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO_-271119/1364
aio_520-24ast_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO_-271119/1365
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO_-271119/1366
aio520-24arr_firmware					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	O-LEN-AIO5-271119/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	O-LEN-AIO5-271119/1368
Linux					
linux_kernel					
Information Exposure	05-11-2019	4	A security issue was discovered in the kube-state-metrics versions v1.7.0 and v1.7.1. An experimental feature was added to the v1.7.0 release that enabled annotations to be exposed as metrics. By default, the kube-state-metrics metrics only expose metadata about Secrets. However, a combination of the default `kubectl` behavior and this new feature can cause the entire secret content to end up in metric labels thus inadvertently exposing the secret content in metrics. This feature has been reverted and released as the v1.7.2 release. If you are running the v1.7.0 or v1.7.1 release, please upgrade to the v1.7.2 release as soon as possible. **CVE ID : CVE-2019-10223**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10223	O-LIN-LINU-271119/1369
NULL Pointer Dereference	04-11-2019	7.8	An issue was discovered in the Linux kernel 4.4.x before 4.4.195. There is a NULL pointer dereference in rds_tcp_kill_sock() in	N/A	O-LIN-LINU-271119/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			net/rds/tcp.c that will cause denial of service, aka CID-91573ae4aed0. **CVE ID : CVE-2019-18680**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	04-11-2019	6.9	An issue was discovered in drivers/media/platform/vivid in the Linux kernel through 5.3.8. It is exploitable for privilege escalation on some Linux distributions where local users have /dev/video0 access, but only if the driver happens to be loaded. There are multiple race conditions during streaming stopping in this driver (part of the V4L2 subsystem). These issues are caused by wrong mutex locking in vivid_stop_generating_vid_cap(), vivid_stop_generating_vid_out(), sdr_cap_stop_streaming(), and the corresponding kthreads. At least one of these race conditions leads to a use-after-free. **CVE ID : CVE-2019-18683**	N/A	O-LIN-LINU-271119/1371
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access	N/A	O-LIN-LINU-271119/1372

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between 7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**		
Information Exposure	06-11-2019	2.1	In the Linux kernel through 5.3.8, f->fmt.sdr.reserved is uninitialized in rcar_drif_g_fmt_sdr_cap in drivers/media/platform/rcar_drif.c, which could cause a memory disclosure problem. **CVE ID : CVE-2019-18786**	N/A	O-LIN-LINU-271119/1373
Integer Overflow or Wraparound	07-11-2019	7.5	An issue was discovered in net/ipv4/sysctl_net_ipv4.c in the Linux kernel before 5.0.11. There is a net/ipv4/tcp_input.c signed integer overflow in tcp_ack_update_rtt() when userspace writes a very large integer to /proc/sys/net/ipv4/tcp_min_rtt_wlen, leading to a denial of service or possibly unspecified other impact, aka CID-19fad20d15a6. **CVE ID : CVE-2019-18805**	N/A	O-LIN-LINU-271119/1374
Uncontrolle	07-11-2019	2.1	A memory leak in the	N/A	O-LIN-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Resource Consumption			ql_alloc_large_buffers() function in drivers/net/ethernet/qlogic/qla3xxx.c in the Linux kernel before 5.3.5 allows local users to cause a denial of service (memory consumption) by triggering pci_dma_mapping_error() failures, aka CID-1acb8f2a7a9f. **CVE ID : CVE-2019-18806**		271119/1375
Uncontrolled Resource Consumption	07-11-2019	5	Two memory leaks in the sja1105_static_config_upload() function in drivers/net/dsa/sja1105/sja1105_spi.c in the Linux kernel before 5.3.5 allow attackers to cause a denial of service (memory consumption) by triggering static_config_buf_prepare_for_upload() or sja1105_inhibit_tx() failures, aka CID-68501df92d11. **CVE ID : CVE-2019-18807**	N/A	O-LIN-LINU-271119/1376
Uncontrolled Resource Consumption	07-11-2019	5	A memory leak in the ccp_run_sha_cmd() function in drivers/crypto/ccp/ccp-ops.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-128c66429247. **CVE ID : CVE-2019-18808**	N/A	O-LIN-LINU-271119/1377
Uncontrolled Resource Consumptio	07-11-2019	7.8	A memory leak in the af9005_identify_state() function in	N/A	O-LIN-LINU-271119/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			drivers/media/usb/dvb-usb/af9005.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-2289adbfa559. **CVE ID : CVE-2019-18809**		
Uncontrolled Resource Consumption	07-11-2019	7.8	A memory leak in the komeda_wb_connector_add() function in drivers/gpu/drm/arm/display/komeda/komeda_wb_connector.c in the Linux kernel before 5.3.8 allows attackers to cause a denial of service (memory consumption) by triggering drm_writeback_connector_init() failures, aka CID-a0ecd6fdbf5d. **CVE ID : CVE-2019-18810**	N/A	O-LIN-LINU-271119/1379
Uncontrolled Resource Consumption	07-11-2019	7.8	A memory leak in the sof_set_get_large_ctrl_data() function in sound/soc/sof/ipc.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering sof_get_ctrl_copy_params() failures, aka CID-45c1380358b1. **CVE ID : CVE-2019-18811**	N/A	O-LIN-LINU-271119/1380
Uncontrolled Resource Consumption	07-11-2019	7.8	A memory leak in the sof_dfsentry_write() function in sound/soc/sof/debug.c in the Linux kernel through 5.3.9 allows attackers to	N/A	O-LIN-LINU-271119/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause a denial of service (memory consumption), aka CID-c0a333d842ef. **CVE ID : CVE-2019-18812**		
Uncontrolled Resource Consumption	07-11-2019	7.8	A memory leak in the dwc3_pci_probe() function in drivers/usb/dwc3/dwc3-pci.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption) by triggering platform_device_add_properties() failures, aka CID-9bbfceea12a8. **CVE ID : CVE-2019-18813**	N/A	O-LIN-LINU-271119/1382
Use After Free	07-11-2019	7.5	An issue was discovered in the Linux kernel through 5.3.9. There is a use-after-free when aa_label_parse() fails in aa_audit_rule_init() in security/apparmor/audit.c. **CVE ID : CVE-2019-18814**	N/A	O-LIN-LINU-271119/1383
Incorrect Default Permissions	12-11-2019	3.6	IBM Spectrum Protect Plus 10.1.0 through 10.1.4 uses insecure file permissions on restored files and directories in Windows which could allow a local user to obtain sensitive information or perform unauthorized actions. IBM X-Force ID: 170963. **CVE ID : CVE-2019-4652**	https://www.ibm.com/support/pages/node/1105683	O-LIN-LINU-271119/1384
mbed					
mbed					
Integer Overflow or	05-11-2019	10	An integer overflow was discovered in the CoAP	N/A	O-MBE-MBED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			library in Arm Mbed OS 5.14.0. The function sn_coap_builder_calc_needed_packet_data_size_2() is used to calculate the required memory for the CoAP message from the sn_coap_hdr_s data structure. Both returned_byte_count and src_coap_msg_ptr->payload_len are of type uint16_t. When added together, the result returned_byte_count can wrap around the maximum uint16_t value. As a result, insufficient buffer space is allocated for the corresponding CoAP message. **CVE ID : CVE-2019-17211**		271119/1385
Out-of-bounds Write	05-11-2019	10	Buffer overflows were discovered in the CoAP library in Arm Mbed OS 5.14.0. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses CoAP input linearly using a while loop. Once an option is parsed in a loop, the current point (*packet_data_pptr) is increased correspondingly. The pointer is restricted by the size of the received buffer, as well as by the 0xFF delimiter byte. Inside each while loop, the check of the	N/A	O-MBE-MBED-271119/1386

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			value of *packet_data_pptr is not strictly enforced. More specifically, inside a loop, *packet_data_pptr could be increased and then dereferenced without checking. Moreover, there are many other functions in the format of sn_coap_parser_****() that do not check whether the pointer is within the bounds of the allocated buffer. All of these lead to heap-based or stack-based buffer overflows, depending on how the CoAP packet buffer is allocated. **CVE ID : CVE-2019-17212**		
Medtronic					
valleylab_ft10_energy_platform_firmware					
Improper Authentication	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism used for authentication between the FT10/LS10 Energy Platform and instruments can be bypassed, allowing for inauthentic instruments to connect to the generator. **CVE ID : CVE-2019-13531**	N/A	O-MED-VALL-271119/1387
Information	08-11-2019	2.1	In Medtronic Valleylab FT10	N/A	O-MED-VALL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism does not apply read protection, allowing for full read access of the RFID security mechanism data. **CVE ID : CVE-2019-13535**		271119/1388
Improper Input Validation	08-11-2019	7.2	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use the descrypt algorithm for OS password hashing. While interactive, network-based logons are disabled, and attackers can use the other vulnerabilities within this report to obtain local shell access and access these hashes. **CVE ID : CVE-2019-13539**	N/A	O-MED-VALL-271119/1389
Use of Hard-coded Credentials	08-11-2019	5	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy	N/A	O-MED-VALL-271119/1390

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Platform (VLFX8GEN) software version 1.1.0 and below use multiple sets of hard-coded credentials. If discovered, they can be used to read files on the device. **CVE ID : CVE-2019-13543**		
valleylab_ls10_energy_platform_firmware					
Improper Authentication	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism used for authentication between the FT10/LS10 Energy Platform and instruments can be bypassed, allowing for inauthentic instruments to connect to the generator. **CVE ID : CVE-2019-13531**	N/A	O-MED-VALL-271119/1391
Information Exposure	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism does not apply read protection, allowing for full read access of the RFID security mechanism data.	N/A	O-MED-VALL-271119/1392

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-13535		
valleylab_fx8_energy_platform_firmware					
Improper Input Validation	08-11-2019	7.2	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use the descrypt algorithm for OS password hashing. While interactive, network-based logons are disabled, and attackers can use the other vulnerabilities within this report to obtain local shell access and access these hashes. **CVE ID : CVE-2019-13539**	N/A	O-MED-VALL-271119/1393
Use of Hard-coded Credentials	08-11-2019	5	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use multiple sets of hard-coded credentials. If discovered, they can be used to read files on the device. **CVE ID : CVE-2019-13543**	N/A	O-MED-VALL-271119/1394
Microsoft					
windows					
Improper Input	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions,	https://nvidia.custhelp	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the size of an input buffer is not validated, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2019-5690**	.com/app/answers/detail/a_id/4907	271119/1395
NULL Pointer Dereference	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which a NULL pointer is dereferenced, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2019-5691**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	O-MIC-WIND-271119/1396
Improper Input Validation	09-11-2019	7.2	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the product uses untrusted input when calculating or using an array index, which may lead to escalation of privileges or denial of service. **CVE ID : CVE-2019-5692**	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	O-MIC-WIND-271119/1397
Access of Uninitialized Pointer	09-11-2019	4.9	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) in which the program accesses or uses a	https://nvidia.custhelp.com/app/answers/detail/a_id/4907	O-MIC-WIND-271119/1398

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer that has not been initialized, which may lead to denial of service. **CVE ID : CVE-2019-5693**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	A Cross Site Scripting (XSS) issue exists in Avast AntiVirus (Free, Internet Security, and Premiere Edition) 19.3.2369 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name. **CVE ID : CVE-2019-18653**	N/A	O-MIC-WIND-271119/1399
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-11-2019	4.3	A Cross Site Scripting (XSS) issue exists in AVG AntiVirus (Internet Security Edition) 19.3.3084 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name. **CVE ID : CVE-2019-18654**	N/A	O-MIC-WIND-271119/1400
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-11-2019	10	An arbitrary command injection vulnerability in the Cluster Server component of Veritas InfoScale allows an unauthenticated remote attacker to execute arbitrary commands as root or administrator. These Veritas products are affected: Access 7.4.2 and earlier, Access Appliance 7.4.2 and earlier, Flex Appliance 1.2 and earlier, InfoScale 7.3.1 and earlier, InfoScale between	N/A	O-MIC-WIND-271119/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.4.0 and 7.4.1, Veritas Cluster Server (VCS) 6.2.1 and earlier on Linux/UNIX, Veritas Cluster Server (VCS) 6.1 and earlier on Windows, Storage Foundation HA (SFHA) 6.2.1 and earlier on Linux/UNIX, and Storage Foundation HA (SFHA) 6.1 and earlier on Windows. **CVE ID : CVE-2019-18780**		
Untrusted Search Path	09-11-2019	4.4	NVIDIA Windows GPU Display Driver, R390 driver version, contains a vulnerability in NVIDIA Control Panel in which it incorrectly loads Windows system DLLs without validating the path or signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution. The attacker requires local system access. **CVE ID : CVE-2019-5694**	N/A	O-MIC-WIND-271119/1402
Untrusted Search Path	12-11-2019	4.4	NVIDIA GeForce Experience (prior to 3.20.1) and Windows GPU Display Driver (all versions) contains a vulnerability in the local service provider component in which an attacker with local system and privileged access can incorrectly load Windows system DLLs without validating the path or	https://nvidia.custhelp.com/app/answers/detail/a_id/4860, https://nvidia.custhelp.com/app/answers/detail/a_id/4907	O-MIC-WIND-271119/1403

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signature (also known as a binary planting or DLL preloading attack), which may lead to denial of service or information disclosure through code execution. **CVE ID : CVE-2019-5695**		
windows_10					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**	N/A	O-MIC-WIND-271119/1404
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1405
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user	N/A	O-MIC-WIND-271119/1406

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0719. **CVE ID : CVE-2019-0721**		
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1407
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'Microsoft Windows Media Foundation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1430**	N/A	O-MIC-WIND-271119/1408
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-271119/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0712, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-1309**		
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1399. **CVE ID : CVE-2019-1310**	N/A	O-MIC-WIND-271119/1410
Information Exposure	12-11-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles IPv6 flowlabel filled in packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1324**	N/A	O-MIC-WIND-271119/1411
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1374**	N/A	O-MIC-WIND-271119/1412
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka	N/A	O-MIC-WIND-271119/1413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1383, CVE-2019-1417. **CVE ID : CVE-2019-1379**		
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1414
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1415
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1416
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-271119/1417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1379, CVE-2019-1417. **CVE ID : CVE-2019-1383**		
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**	N/A	O-MIC-WIND-271119/1418
Improper Privilege Managemen t	12-11-2019	6.1	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1385**	N/A	O-MIC-WIND-271119/1419
Improper Privilege Managemen	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog	N/A	O-MIC-WIND-271119/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**		
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**	N/A	O-MIC-WIND-271119/1421
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1422
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1423
Improper Privilege Managemen	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to	N/A	O-MIC-WIND-271119/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1392**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1425
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1426
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-	N/A	O-MIC-WIND-271119/1427

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1428
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1429
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1397.	N/A	O-MIC-WIND-271119/1430

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1398		
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**	N/A	O-MIC-WIND-271119/1431
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1432
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1433
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics	N/A	O-MIC-WIND-271119/1434

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1435
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1436
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1437

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	4.3	A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls, aka 'Microsoft Edge Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1413**	N/A	O-MIC-WIND-271119/1438
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1439
Improper Privilege Managemen t	12-11-2019	4.4	An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1416**	N/A	O-MIC-WIND-271119/1440
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-271119/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1379, CVE-2019-1383. **CVE ID : CVE-2019-1417**		
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1442
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**	N/A	O-MIC-WIND-271119/1443
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1444
Improper Privilege	12-11-2019	4.6	An elevation of privilege vulnerability exists in the	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**		271119/1445
Improper Privilege Management	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the StartTileData.dll handles file creation in protected locations, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1422. **CVE ID : CVE-2019-1423**	N/A	O-MIC-WIND-271119/1446
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1426**	N/A	O-MIC-WIND-271119/1447
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-271119/1448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1426, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1427**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429. **CVE ID : CVE-2019-1428**	N/A	O-MIC-WIND-271119/1449
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1450
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438.	N/A	O-MIC-WIND-271119/1451

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1433		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**	N/A	O-MIC-WIND-271119/1452
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1453
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1440. **CVE ID : CVE-2019-1436**	N/A	O-MIC-WIND-271119/1454
Improper Privilege	12-11-2019	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-271119/1455

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1438. **CVE ID : CVE-2019-1437**		
Improper Privilege Management	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**	N/A	O-MIC-WIND-271119/1456
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1457
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-271119/1458

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1436. **CVE ID : CVE-2019-1440**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1459
windows_7					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**	N/A	O-MIC-WIND-271119/1460
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-271119/1461

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**		
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1462
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1411. **CVE ID : CVE-2019-1432**	N/A	O-MIC-WIND-271119/1463
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1464
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege	N/A	O-MIC-WIND-271119/1465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-1382**		
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**	N/A	O-MIC-WIND-271119/1466
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1467
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**	N/A	O-MIC-WIND-271119/1468
Improper Restriction of	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine	N/A	O-MIC-WIND-271119/1469

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**		
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1470
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1471
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1472
Improper	12-11-2019	7.2	An elevation of privilege	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**		271119/1473
Improper Privilege Management	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1474
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1475
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host	N/A	O-MIC-WIND-271119/1476

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1477
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1478
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435,	N/A	O-MIC-WIND-271119/1479

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1480
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1481
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1482
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver	N/A	O-MIC-WIND-271119/1483

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(ATMFD.dll) when it fails to properly handle objects in memory, aka 'OpenType Font Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1412**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1484
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1485
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-271119/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1456. **CVE ID : CVE-2019-1419**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1487
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**	N/A	O-MIC-WIND-271119/1488
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1489
Improper Privilege Managemen	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly	N/A	O-MIC-WIND-271119/1490

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**	N/A	O-MIC-WIND-271119/1491
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1492
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly	N/A	O-MIC-WIND-271119/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1494
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Win32k Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1441**	N/A	O-MIC-WIND-271119/1495
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1496

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
windows_8.1					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**	N/A	O-MIC-WIND-271119/1497
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1498
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1499
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its	N/A	O-MIC-WIND-271119/1500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1411. **CVE ID : CVE-2019-1432**		
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1501
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1502
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1503
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication	N/A	O-MIC-WIND-271119/1504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1505
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**	N/A	O-MIC-WIND-271119/1506
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1507
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of	N/A	O-MIC-WIND-271119/1508

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1392**	N/A	O-MIC-WIND-271119/1509
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1510
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1511
Improper Privilege Managemen	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k	N/A	O-MIC-WIND-271119/1512

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1513
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1514
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a	N/A	O-MIC-WIND-271119/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1516
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1517
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438.	N/A	O-MIC-WIND-271119/1518

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1407		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1519
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1520
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1521
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in	N/A	O-MIC-WIND-271119/1522

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'OpenType Font Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1412**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1523
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1524
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**	N/A	O-MIC-WIND-271119/1525

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1526
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**	N/A	O-MIC-WIND-271119/1527
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1528
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics	N/A	O-MIC-WIND-271119/1529

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**	N/A	O-MIC-WIND-271119/1530
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1531
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics	N/A	O-MIC-WIND-271119/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1533
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1534
windows_rt_8.1					
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1535

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1411. **CVE ID : CVE-2019-1432**	N/A	O-MIC-WIND-271119/1536
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1537
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1538
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1539
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and	N/A	O-MIC-WIND-271119/1540

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1541
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1542
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1543
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows	N/A	O-MIC-WIND-271119/1544

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1392**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1545
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1546
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**	N/A	O-MIC-WIND-271119/1547

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1548
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1549
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1550
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-271119/1551

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1552
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1553
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1554
Information	12-11-2019	2.1	An information disclosure vulnerability exists in	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory, aka 'OpenType Font Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1412**		271119/1555
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1556
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1557
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution	N/A	O-MIC-WIND-271119/1558

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1559
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**	N/A	O-MIC-WIND-271119/1560
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1561
Improper Privilege	12-11-2019	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**		271119/1562
Improper Privilege Management	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**	N/A	O-MIC-WIND-271119/1563
Improper Privilege Management	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1564
Improper Privilege	12-11-2019	7.2	An elevation of privilege vulnerability exists when the	N/A	O-MIC-WIND-271119/1565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1566
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1567
windows_server_2008					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a	N/A	O-MIC-WIND-271119/1568

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**		
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1569
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1570
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1411. **CVE ID : CVE-2019-1432**	N/A	O-MIC-WIND-271119/1571

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1572
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**	N/A	O-MIC-WIND-271119/1573
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1574
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution	N/A	O-MIC-WIND-271119/1575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1576
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1577
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1578
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of	N/A	O-MIC-WIND-271119/1579

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**	N/A	O-MIC-WIND-271119/1580
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1581
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution	N/A	O-MIC-WIND-271119/1582

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**		
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**	N/A	O-MIC-WIND-271119/1583
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1584
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1585
Improper Privilege Managemen	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics	N/A	O-MIC-WIND-271119/1586

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1587
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1588
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is	N/A	O-MIC-WIND-271119/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**		
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory, aka 'OpenType Font Driver Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1412**	N/A	O-MIC-WIND-271119/1590
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1591
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1592
Improper Restriction of Operations	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type	N/A	O-MIC-WIND-271119/1593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**	N/A	O-MIC-WIND-271119/1594
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1595
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-271119/1596

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**	N/A	O-MIC-WIND-271119/1597
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1598
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-271119/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**		
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1600
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts, aka 'Win32k Graphics Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1441**	N/A	O-MIC-WIND-271119/1601
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1602
windows_server_2012					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network	N/A	O-MIC-WIND-271119/1603

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**		
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1604
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1605
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-271119/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1411. **CVE ID : CVE-2019-1432**		
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1607
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1608
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1609
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'.	N/A	O-MIC-WIND-271119/1610

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1384		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1611
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**	N/A	O-MIC-WIND-271119/1612
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1613
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207.	N/A	O-MIC-WIND-271119/1614

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1391		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1392**	N/A	O-MIC-WIND-271119/1615
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1616
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1617
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of	N/A	O-MIC-WIND-271119/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1619
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1620
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of	N/A	O-MIC-WIND-271119/1621

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1622
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1623
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**	N/A	O-MIC-WIND-271119/1624
Improper Privilege	12-11-2019	7.2	An elevation of privilege vulnerability exists in	N/A	O-MIC-WIND-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**		271119/1625
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1626
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1627
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists in Windows Adobe Type Manager Font Driver (ATMFD.dll) when it fails to properly handle objects in memory, aka 'OpenType Font Driver Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-271119/1628

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1412		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1629
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1630
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**	N/A	O-MIC-WIND-271119/1631
Improper Privilege Managemen	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll	N/A	O-MIC-WIND-271119/1632

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1633
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**	N/A	O-MIC-WIND-271119/1634
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-271119/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408. **CVE ID : CVE-2019-1434**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1636
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**	N/A	O-MIC-WIND-271119/1637
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1638

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1639
windows_server_2016					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**	N/A	O-MIC-WIND-271119/1640
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1641

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0719. **CVE ID : CVE-2019-0721**	N/A	O-MIC-WIND-271119/1642
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1643
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when Windows Media Foundation improperly parses specially crafted QuickTime media files.An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'Microsoft Windows Media Foundation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1430**	N/A	O-MIC-WIND-271119/1644
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails	N/A	O-MIC-WIND-271119/1645

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-1309**		
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1399. **CVE ID : CVE-2019-1310**	N/A	O-MIC-WIND-271119/1646
Information Exposure	12-11-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles IPv6 flowlabel filled in packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1324**	N/A	O-MIC-WIND-271119/1647
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-271119/1648

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1374		
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1649
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1650
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1651
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1379, CVE-2019-1417. **CVE ID : CVE-2019-1383**	N/A	O-MIC-WIND-271119/1652
Improper	12-11-2019	6.5	A security feature bypass	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1384**		271119/1653
Improper Privilege Managemen t	12-11-2019	6.1	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1385**	N/A	O-MIC-WIND-271119/1654
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-271119/1655

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1388		
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1397, CVE-2019-1398. **CVE ID : CVE-2019-1389**	N/A	O-MIC-WIND-271119/1656
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1657
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1658
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-	N/A	O-MIC-WIND-271119/1659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1660
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**	N/A	O-MIC-WIND-271119/1661
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434.	N/A	O-MIC-WIND-271119/1662

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1396		
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1663
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1397. **CVE ID : CVE-2019-1398**	N/A	O-MIC-WIND-271119/1664
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310.	N/A	O-MIC-WIND-271119/1665

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1399		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1666
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1667
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1433, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1407**	N/A	O-MIC-WIND-271119/1668
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of	N/A	O-MIC-WIND-271119/1669

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**		
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1670
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1671
Improper Input Validation	12-11-2019	4.3	A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls, aka 'Microsoft Edge Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1413**	N/A	O-MIC-WIND-271119/1672
Improper Privilege Managemen	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because	N/A	O-MIC-WIND-271119/1673

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**		
Improper Privilege Managemen t	12-11-2019	4.4	An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1416**	N/A	O-MIC-WIND-271119/1674
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1379, CVE-2019-1383. **CVE ID : CVE-2019-1417**	N/A	O-MIC-WIND-271119/1675
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**	N/A	O-MIC-WIND-271119/1676

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
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**	N/A	O-MIC-WIND-271119/1677
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1678
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423. **CVE ID : CVE-2019-1422**	N/A	O-MIC-WIND-271119/1679
Improper Restriction of Operations	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory	N/A	O-MIC-WIND-271119/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1426**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429. **CVE ID : CVE-2019-1428**	N/A	O-MIC-WIND-271119/1681
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**	N/A	O-MIC-WIND-271119/1682
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This	N/A	O-MIC-WIND-271119/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1684
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1440. **CVE ID : CVE-2019-1436**	N/A	O-MIC-WIND-271119/1685
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-	N/A	O-MIC-WIND-271119/1686

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1438. **CVE ID : CVE-2019-1437**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**	N/A	O-MIC-WIND-271119/1687
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1439**	N/A	O-MIC-WIND-271119/1688
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436. **CVE ID : CVE-2019-1440**	N/A	O-MIC-WIND-271119/1689
Improper Restriction of Operations within the Bounds of a	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted	N/A	O-MIC-WIND-271119/1690

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**		
windows_server_2019					
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1309, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-0712**	N/A	O-MIC-WIND-271119/1691
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0721. **CVE ID : CVE-2019-0719**	N/A	O-MIC-WIND-271119/1692
Improper Input Validation	12-11-2019	9	A remote code execution vulnerability exists when Windows Hyper-V Network Switch on a host server fails to properly validate input from an authenticated user	N/A	O-MIC-WIND-271119/1693

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on a guest operating system, aka 'Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0719. **CVE ID : CVE-2019-0721**		
Improper Input Validation	12-11-2019	6.8	A security feature bypass vulnerability exists when Windows Netlogon improperly handles a secure communications channel, aka 'NetLogon Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1424**	N/A	O-MIC-WIND-271119/1694
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1310, CVE-2019-1399. **CVE ID : CVE-2019-1309**	N/A	O-MIC-WIND-271119/1695
Improper Input Validation	12-11-2019	6.8	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309,	N/A	O-MIC-WIND-271119/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-1399. **CVE ID : CVE-2019-1310**		
Information Exposure	12-11-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles IPv6 flowlabel filled in packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1324**	N/A	O-MIC-WIND-271119/1697
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists in the way Windows Error Reporting (WER) handles objects in memory, aka 'Windows Error Reporting Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1374**	N/A	O-MIC-WIND-271119/1698
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1383, CVE-2019-1417. **CVE ID : CVE-2019-1379**	N/A	O-MIC-WIND-271119/1699
Improper Privilege Managemen t	12-11-2019	4.6	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1380**	N/A	O-MIC-WIND-271119/1700

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Servicing Stack allows access to unprivileged file locations, aka 'Microsoft Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1381**	N/A	O-MIC-WIND-271119/1701
Improper Privilege Managemen t	12-11-2019	2.1	An elevation of privilege vulnerability exists when ActiveX Installer service may allow access to files without proper authentication, aka 'Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1382**	N/A	O-MIC-WIND-271119/1702
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1379, CVE-2019-1417. **CVE ID : CVE-2019-1383**	N/A	O-MIC-WIND-271119/1703
Improper Input Validation	12-11-2019	6.5	A security feature bypass vulnerability exists where a NETLOGON message is able to obtain the session key and sign messages.To exploit this vulnerability, an attacker could send a specially crafted authentication request, aka 'Microsoft Windows Security Feature	N/A	O-MIC-WIND-271119/1704

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bypass Vulnerability'. **CVE ID : CVE-2019-1384**		
Improper Privilege Managemen t	12-11-2019	6.1	An elevation of privilege vulnerability exists when the Windows AppX Deployment Extensions improperly performs privilege management, resulting in access to system files.To exploit this vulnerability, an authenticated attacker would need to run a specially crafted application to elevate privileges.The security update addresses the vulnerability by correcting how AppX Deployment Extensions manages privileges., aka 'Windows AppX Deployment Extensions Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1385**	N/A	O-MIC-WIND-271119/1705
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in the Windows Certificate Dialog when it does not properly enforce user privileges, aka 'Windows Certificate Dialog Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1388**	N/A	O-MIC-WIND-271119/1706
Improper Restriction of Operations within the Bounds of a Memory	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1390**	N/A	O-MIC-WIND-271119/1707

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
Improper Input Validation	12-11-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2018-12207. **CVE ID : CVE-2019-1391**	N/A	O-MIC-WIND-271119/1708
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1393**	N/A	O-MIC-WIND-271119/1709
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1395, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1394**	N/A	O-MIC-WIND-271119/1710
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory,	N/A	O-MIC-WIND-271119/1711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1396, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1395**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1408, CVE-2019-1434. **CVE ID : CVE-2019-1396**	N/A	O-MIC-WIND-271119/1712
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1398. **CVE ID : CVE-2019-1397**	N/A	O-MIC-WIND-271119/1713
Improper Input Validation	12-11-2019	7.7	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka	N/A	O-MIC-WIND-271119/1714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Hyper-V Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1389, CVE-2019-1397. **CVE ID : CVE-2019-1398**		
Improper Input Validation	12-11-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0712, CVE-2019-1309, CVE-2019-1310. **CVE ID : CVE-2019-1399**	N/A	O-MIC-WIND-271119/1715
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Universal Plug and Play (UPnP) service improperly allows COM object creation, aka 'Windows UPnP Service Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1405**	N/A	O-MIC-WIND-271119/1716
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-1406**	N/A	O-MIC-WIND-271119/1717

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1393, CVE-2019-1394, CVE-2019-1395, CVE-2019-1396, CVE-2019-1434. **CVE ID : CVE-2019-1408**	N/A	O-MIC-WIND-271119/1718
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the Windows Remote Procedure Call (RPC) runtime improperly initializes objects in memory, aka 'Windows Remote Procedure Call Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1409**	N/A	O-MIC-WIND-271119/1719
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1432. **CVE ID : CVE-2019-1411**	N/A	O-MIC-WIND-271119/1720
Improper Input Validation	12-11-2019	4.3	A security feature bypass vulnerability exists when Microsoft Edge improperly handles extension requests and fails to request host permission for all_urls, aka 'Microsoft Edge Security	N/A	O-MIC-WIND-271119/1721

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability'. **CVE ID : CVE-2019-1413**		
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in Windows Installer because of the way Windows Installer handles certain filesystem operations.To exploit the vulnerability, an attacker would require unprivileged execution on the victim system, aka 'Windows Installer Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1415**	N/A	O-MIC-WIND-271119/1722
Improper Privilege Managemen t	12-11-2019	4.4	An elevation of privilege vulnerability exists due to a race condition in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-1416**	N/A	O-MIC-WIND-271119/1723
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1379, CVE-2019-1383. **CVE ID : CVE-2019-1417**	N/A	O-MIC-WIND-271119/1724
Information Exposure	12-11-2019	2.1	An information vulnerability exists when Windows Modules Installer Service improperly discloses file	N/A	O-MIC-WIND-271119/1725

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'. **CVE ID : CVE-2019-1418**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1456. **CVE ID : CVE-2019-1419**	N/A	O-MIC-WIND-271119/1726
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1422, CVE-2019-1423. **CVE ID : CVE-2019-1420**	N/A	O-MIC-WIND-271119/1727
Improper Privilege Managemen t	12-11-2019	4.6	An elevation of privilege vulnerability exists in the way that the iphlpsvc.dll handles file creation allowing for a file overwrite, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1420, CVE-2019-1423.	N/A	O-MIC-WIND-271119/1728

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1422		
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1427, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1426**	N/A	O-MIC-WIND-271119/1729
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1428, CVE-2019-1429. **CVE ID : CVE-2019-1427**	N/A	O-MIC-WIND-271119/1730
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge (HTML-based), aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1429. **CVE ID : CVE-2019-1428**	N/A	O-MIC-WIND-271119/1731
Improper Restriction	12-11-2019	7.6	A remote code execution vulnerability exists in the	N/A	O-MIC-WIND-271119/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1426, CVE-2019-1427, CVE-2019-1428. **CVE ID : CVE-2019-1429**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1435, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1433**	N/A	O-MIC-WIND-271119/1733
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1437, CVE-2019-1438. **CVE ID : CVE-2019-1435**	N/A	O-MIC-WIND-271119/1734
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel	N/A	O-MIC-WIND-271119/1735

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1440. **CVE ID : CVE-2019-1436**		
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1438. **CVE ID : CVE-2019-1437**	N/A	O-MIC-WIND-271119/1736
Improper Privilege Managemen t	12-11-2019	7.2	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1407, CVE-2019-1433, CVE-2019-1435, CVE-2019-1437. **CVE ID : CVE-2019-1438**	N/A	O-MIC-WIND-271119/1737
Information Exposure	12-11-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	N/A	O-MIC-WIND-271119/1738

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1439		
Information Exposure	12-11-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1436. **CVE ID : CVE-2019-1440**	N/A	O-MIC-WIND-271119/1739
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-11-2019	6.8	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles specially crafted OpenType fonts, aka 'OpenType Font Parsing Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1419. **CVE ID : CVE-2019-1456**	N/A	O-MIC-WIND-271119/1740
Opensuse					
leap					
Weak Password Requirements	06-11-2019	4.9	A flaw was found in Samba, all versions starting samba 4.5.0 before samba 4.9.15, samba 4.10.10, samba 4.11.2, in the way it handles a user password change or a new password for a samba user. The Samba Active Directory Domain Controller can be configured to use a custom script to check for password complexity. This configuration can fail to	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14833	O-OPE-LEAP-271119/1741

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verify password complexity when non-ASCII characters are used in the password, which could lead to weak passwords being set for samba users, making it vulnerable to dictionary attacks. **CVE ID : CVE-2019-14833**		
NULL Pointer Dereference	06-11-2019	4	A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue. **CVE ID : CVE-2019-14847**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14847	O-OPE-LEAP-271119/1742
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source,	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensuse-security-announce/2019-10/msg00048.html	O-OPE-LEAP-271119/1743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**		
patriotmemory					
viper_rgb_firmware					
Improper Privilege Managemen t	09-11-2019	3.6	The MsIo64.sys and MsIo32.sys drivers in Patriot Viper RGB before 1.1 allow local users (including low integrity processes) to read and write to arbitrary memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, by mapping \Device\PhysicalMemory into the calling process via	N/A	O-PAT-VIPE-271119/1744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZwOpenSection and ZwMapViewOfSection. **CVE ID : CVE-2019-18845**		
Qualcomm					
qca6574au_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1745
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1747

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1748
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1749

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850,	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20 **CVE ID : CVE-2019-10542**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1751
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
qcs405_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1753
Out-of-bounds	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request	https://source.android.com/securit	O-QUA-QCS4-271119/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1755

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1756

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1757
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1758

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1759
Concurrent Execution using Shared Resource with	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1760

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Synchronization ('Race Condition')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1761

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1762
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1764
Integer Overflow or	06-11-2019	7.5	While processing vendor command which contains	https://source.android.	O-QUA-QCS4-271119/1765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	com/security/bulletin/	
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1766

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

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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1767

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-10491**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1768
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1769

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1770

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-QCS4-271119/1771
sd_665_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1772

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1773
Uncontrolle	06-11-2019	5	Firmware not able to send	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Resource Consumption			EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	rce.android.com/security/bulletin/	271119/1774
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1775

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 650/52, 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-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1776
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring	https://source.android.com/securit	O-QUA-SD_6-271119/1777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	y/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1778

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1779
Concurrent Execution using Shared Resource with	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1780

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Synchronization ('Race Condition')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1781

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1782
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1783

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1784

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1785
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1786

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

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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1787

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10488		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1788
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1789

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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1790

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1791
Improper Restriction of Operations within the	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1793

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1794
Improper Restriction of Operations	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1795

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_730_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1796

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1797
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1798

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1799

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1800
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 /	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1802

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1803
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1804

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1805

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1806
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1808
Out-of-bounds	06-11-2019	10	Kernel can do a memory read from arbitrary address	https://source.android.	O-QUA-SD_7-271119/1809

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1811
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1812

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1813

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

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, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1814
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	O-QUA-SD_7-271119/1815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1816

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1817

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1818
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1819

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/1820

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
ipq4019_firmware					
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-IPQ4-271119/1821
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-IPQ4-271119/1822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
ipq8064_firmware					
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-IPQ8-271119/1823

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-IPQ8-271119/1824

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, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
ipq8074_firmware					
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-IPQ8-271119/1825
Out-of-bounds	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during	https://source.android.com/securit	O-QUA-IPQ8-271119/1826

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	y/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-IPQ8-271119/1827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
qca6174a_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1829
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qca9377_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1831

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10505		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1832
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053,	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1833

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qca9379_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1834

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1835
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-QCA9-271119/1836

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sd616_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SD61-271119/1837

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, SDX24 **CVE ID : CVE-2019-10491**		
apq8053_firmware					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-APQ8-271119/1838
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-APQ8-271119/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
mdm9207c_firmware					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1840
Integer Overflow or Wraparoun	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and	https://source.android.com/securit	O-QUA-MDM9-271119/1841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	y/bulletin/	
msm8905_firmware					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1843
qcn7605_firmware					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-QCN7-271119/1844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-QCN7-271119/1845
sdm845_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-SDM8-271119/1846
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://source.android.com/security/bulletin/	O-QUA-SDM8-271119/1847

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
apq8017_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-APQ8-271119/1848
apq8096au_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and	https://source.android.com/security/bulletin/	O-QUA-APQ8-271119/1849

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
msm8976_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sda845_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-SDA8-271119/1851

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm636_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/1852
sdm670_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/1853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sdm710_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845,	https://source.android.com/security/bulletin/	O-QUA-SDM7-271119/1854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sm6150_firmware					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-SM61-271119/1855
sd_600_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1857

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1858
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1859

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 Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1860

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10542		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1861
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1862

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
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1863

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
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/1864
qca6574_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-QCA6-271119/1865

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
qca8081_firmware					
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-QCA8-271119/1866

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcs404_firmware					
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS4-271119/1867
sm8150_firmware					
Integer	06-11-2019	7.5	While processing vendor	https://sou	O-QUA-SM81-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	rce.android.com/security/bulletin/	271119/1868
mdm9206_firmware					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1869

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1870
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1872

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1873
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1874

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1875

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1876
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1877

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1878

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1879
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1880

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1881
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1882

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1883

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1884
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1885

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-271119/1886

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1887

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1888
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1889

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1890

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1891
mdm9607_firmware					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1892

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1894
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1896

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1897
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1898

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1899

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1900
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1901
NULL	06-11-2019	10	Null-pointer dereference can	https://sou	O-QUA-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	rce.android.com/security/bulletin/	MDM9-271119/1902
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1903

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1904
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1905

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 Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1906

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1907
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1910
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key	https://www.qualcomm.com/company/produ	O-QUA-MDM9-271119/1911

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	ct-security/bulletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1912

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1913

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1914
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1915

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1916

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
mdm9650_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1917
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/securit	O-QUA-MDM9-271119/1918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	y/bulletin/	
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1919

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10515**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1920
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its	https://source.android.com/securit	O-QUA-MDM9-271119/1921

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	y/bulletin/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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 /	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1922

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1923
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1925

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1926
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1927

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1929
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key	https://www.qualcomm.com/company/produ	O-QUA-MDM9-271119/1930

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	ct-security/bulletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1931

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1932

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1933
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1935

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
mdm9655_firmware					
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/1936

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msm8996au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1937
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1938

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1939

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1940
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1941

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1942

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1943
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1944

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1945
NULL	06-11-2019	10	Null-pointer dereference can	https://sou	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	rce.android.com/security/bulletin/	MSM8-271119/1946
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1947

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1948
Improper Restriction of Operations within the Bounds of a	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1950

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1951
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1952

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1953

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1954
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC	https://source.android.com/securit	O-QUA-MSM8-271119/1955

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encoding. 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-2019-10495**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1956

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

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-271119/1957

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1958
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1959

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1960

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

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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/1961

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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_410_firmware					
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-271119/1962
sd_412_firmware					
Improper	06-11-2019	2.1	While deserializing any key	https://ww	O-QUA-SD_4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	w.qualcomm.com/company/product-security/bulletins	271119/1963
sd_820a_firmware					
Buffer Copy without Checking	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data	https://source.android.com/securit	O-QUA-SD_8-271119/1964

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			structure leads to buffer overflow 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-2019-10496**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1965

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1966

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1967
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1968

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1969

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1970
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1971

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1972
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1973

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1974

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1975
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1976

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1977

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1978
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1979

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1980

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1981
Improper	06-11-2019	2.1	While deserializing any key	https://ww	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	w.qualcomm.com/company/product-security/bulletins	271119/1982
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1983

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1984

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1985
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1986

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/1987

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
qualcomm_215_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1988
Buffer Copy without Checking	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in	https://source.android.com/securit	O-QUA-QUAL-271119/1989

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	y/bulletin/	
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1990
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1991

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1992

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1993
Concurrent Execution	06-11-2019	9.3	Possible use after free issue due to race condition while	https://source.android.	O-QUA-QUAL-271119/1994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1995
Improper	06-11-2019	10	Out of bound access due to	https://sou	O-QUA-QUAL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	rce.android.com/security/bulletin/	271119/1996
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1997

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1998
Improper Restriction of Operations within the	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/1999

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2000

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2001
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2003

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2004
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory	https://source.android.com/securit	O-QUA-QUAL-271119/2005

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	y/bulletin/	
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QUAL-271119/2006

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2007

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2008
Integer Overflow or	06-11-2019	10	Possible Integer overflow because of subtracting two	https://source.android.	O-QUA-QUAL-271119/2009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-QUAL-271119/2010

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_205_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2011

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2012
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2013

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10504		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2014
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2015

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2016

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2017
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2018

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2019
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	O-QUA-SD_2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/2020
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2021

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2022
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2023

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

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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2024
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2025

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2026

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2027
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2028

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2029

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

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, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2030
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	O-QUA-SD_2-271119/2031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-271119/2032

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2033

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

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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2034
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2035

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2036

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

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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2037

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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_210_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2038
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2040
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2041

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2042

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2045

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2046
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2047

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2048
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2049

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

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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2050
Improper Restriction of	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with	https://source.android.com/securit	O-QUA-SD_2-271119/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2052

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2053
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2054

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2055

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2056
Improper Input	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence	https://source.android.	O-QUA-SD_2-271119/2057

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			header during HEVC or AVC encoding. 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-2019-10495**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2058

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

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-271119/2059

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2060
Improper Restriction of	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might	https://source.android.com/securit	O-QUA-SD_2-271119/2061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2063
Improper Restriction	06-11-2019	10	Memory corruption while accessing the memory as	https://source.android.	O-QUA-SD_2-271119/2064

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	com/security/bulletin/	
sd_212_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2066
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2069
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2070

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2071

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2072
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2074
Buffer Copy	06-11-2019	10	Incorrect reading of system	https://sou	O-QUA-SD_2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	rce.android.com/security/bulletin/	271119/2075
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2076
NULL Pointer	06-11-2019	10	Null-pointer dereference can occur while accessing the	https://source.android.	O-QUA-SD_2-271119/2077

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2078

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2079
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2080

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2081

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2082
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2083

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2084

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

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2085

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_2-271119/2086
N/A	06-11-2019	10	Lack of check to ensure	https://sou	O-QUA-SD_2-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	rce.android.com/security/bulletin/	271119/2087
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2088

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

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 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2089
Integer Overflow or Wraparoun	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if	https://source.android.com/securit	O-QUA-SD_2-271119/2090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	y/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-SD_2-271119/2091

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
sd_415_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2093
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2094

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2095

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2096
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2097

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2098

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2099

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2324		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2100
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2101

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2102

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332**		
sd_425_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2103
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2105
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2106

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2107

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2108
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2110

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2111
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2112

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2113
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2114

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2115

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2116
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2117

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2118
Improper Restriction of	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating	https://source.android.com/securit	O-QUA-SD_4-271119/2119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			pointer can lead to out-of-bound access 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, 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 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-2019-2283**	y/bulletin/	
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2120

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

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2121
Buffer Copy without	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose	https://source.android.	O-QUA-SD_4-271119/2122

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	com/security/bulletin/	
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2123

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2124

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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_4-271119/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			, SXR1130 **CVE ID : CVE-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2126
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2127

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2128

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2129
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_427_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2131

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2132
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2133

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2134

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10515		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2135
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2136

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2137
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2138

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2139

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10534**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2140
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2141

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2142

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2143
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2144

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

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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2145

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10488		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2146
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2147

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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2148

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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_4-271119/2149

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2150
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2151

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2153
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2154

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_429_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2155

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, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2156
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2157

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2158
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2159

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2160

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2161
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2162

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2163

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2164
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2165

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			439 / SD 429, SD 450, SD 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2166
Improper Restriction of Operations within the	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2167

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, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2168

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2169
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2170

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2171

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2172
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2173

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2174

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-271119/2175

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2176
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2177

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2178

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2179
sd_430_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2180
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2181

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2182
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2183

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2184

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2185
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2187

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10533		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2188
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2189

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2190
Out-of-bounds	06-11-2019	10	Out of bound write issue is observed while giving	https://source.android.	O-QUA-SD_4-271119/2191

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			information about properties that have been set so far for playing video 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-2019-2285**	com/security/bulletin/	
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2192

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2193

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2194
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2195

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-271119/2196

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2197

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2198
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2199

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2201
sd_435_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2202

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2203
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	O-QUA-SD_4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	271119/2204
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2205

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2206
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	O-QUA-SD_4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	271119/2207
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2208

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

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 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2209
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2210

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2211

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2212
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2213

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2214
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about	https://source.android.com/securit	O-QUA-SD_4-271119/2215

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properties that have been set so far for playing video 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-2019-2285**	y/bulletin/	
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2216

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

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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2217

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2218
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2219

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-271119/2220

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2221

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2222
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2223

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2224

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2225
sd_439_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2226

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2227
Uncontrolled Resource	06-11-2019	5	Firmware not able to send EXT scan response to host	https://source.android.	O-QUA-SD_4-271119/2228

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	com/security/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2229

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2230
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2231

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2232

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2233
Concurrent Execution using Shared Resource with Improper	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2235
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2236

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2237

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2238
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2239

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2240

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2283		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2241
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2242

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2243

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2244
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2245

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_4-271119/2246

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2247

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2248
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2249

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2250

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
sd_450_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2251
Buffer Copy without	06-11-2019	4.6	Possible stack overflow when an index equal to io	https://source.android.	O-QUA-SD_4-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	com/security/bulletin/	271119/2252
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2253
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request	https://source.android.com/securit	O-QUA-SD_4-271119/2254

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2255

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2257
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2258

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2259
Concurrent Execution using Shared Resource with	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2260

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Synchronization ('Race Condition')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2261
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2262

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2263

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2264
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2266

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2267
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2268

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

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 625, SD 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2269
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	O-QUA-SD_4-271119/2270

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2271

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2272

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2273
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_4-271119/2274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	lletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2275

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2276

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2324		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2277
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2278

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_4-271119/2279

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332**		
sd_615_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2280
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2281

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2282

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2283
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	O-QUA-SD_6-271119/2284

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2285

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2287
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2289

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

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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2290
mdm9615_firmware					
Out-of-bounds	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that	https://source.android.com/securit	O-QUA-MDM9-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	y/bulletin/	271119/2291
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2292

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2293
Integer Overflow or	06-11-2019	10	Possible Integer overflow because of subtracting two	https://source.android.	O-QUA-MDM9-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	com/security/bulletin/	271119/2294
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2295

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2332**		
mdm9625_firmware					
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
mdm9205_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2297
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2298

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-271119/2299

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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 712 / SD 710 / SD 670, 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-2019-2275**		
msm8909_firmware					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2300
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
mdm9635m_firmware					
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2302

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2258**		
sd_616_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2304
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2305

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2306

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2307
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2308

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2309

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2310
Integer Overflow or	06-11-2019	10	Possible Integer overflow because of subtracting two	https://source.android.	O-QUA-SD_6-271119/2311

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2312

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_625_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2313

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2314
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2315

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10504		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2316
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2317

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2318

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2319
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2320

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2321
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	O-QUA-SD_6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/2322
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2323

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2324
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2325

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

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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2326
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2327

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2328

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2329
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2330

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2331

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2332
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2333

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2334

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2335
Improper Input	06-11-2019	2.1	While deserializing any key blob during key operations,	https://www.qualcom	O-QUA-SD_6-271119/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	m.com/company/product-security/bulletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2337

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2338

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2339
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2340

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2341

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

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, SDX24 **CVE ID : CVE-2019-2332**		
sd_632_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2342
Buffer Copy without Checking Size of Input	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in	https://source.android.com/securit	O-QUA-SD_6-271119/2343

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	y/bulletin/	
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2344
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2345

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2346

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2347
Buffer Copy without	06-11-2019	7.5	While playing the clip which is nonstandard buffer	https://source.android.	O-QUA-SD_6-271119/2348

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	com/security/bulletin/	
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2349

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2350
Buffer Copy without	06-11-2019	10	Incorrect reading of system image resulting in buffer	https://source.android.	O-QUA-SD_6-271119/2351

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2352
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is	https://source.android.com/securit	O-QUA-SD_6-271119/2353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	y/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2354

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2355
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2356

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2357

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2358
Improper	06-11-2019	4.6	Arbitrary buffer write issue	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	rce.android.com/security/bulletin/	271119/2359
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2360

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-271119/2361

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2362
Improper Validation of	06-11-2019	10	Out of boundary access due to token received from ADSP	https://source.android.	O-QUA-SD_6-271119/2363

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	com/security/bulletin/	
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2364

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2365

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2332**		
sd_636_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2366
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2367

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2368
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	271119/2369
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2370

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2371
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	271119/2372
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2373

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

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 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2374
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2375

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2376

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2377
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2378

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2379
Improper	06-11-2019	10	Improper validation of read	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	rce.android.com/security/bulletin/	271119/2380
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2381

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2382

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2383
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2384

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2385

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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_6-271119/2386

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2387
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2388

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2389

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2390
sd_650_firmware					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2391

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2392

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2393
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_6-271119/2394

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	lletins	
sd_652_firmware					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10505		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2397
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_6-271119/2398

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
sda660_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2399

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-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2400
Out-of-bounds	06-11-2019	7.5	Out of bound access while processing a non-standard	https://source.android.	O-QUA-SDA6-271119/2401

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2402

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10515		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2404
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2405

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2406
Concurrent Execution using Shared	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2407

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2408

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			439 / SD 429, SD 450, SD 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2409
Improper Restriction of Operations within the	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2410

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, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2411

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2412
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2413

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2414

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2416

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2417

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2418
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur	https://www.qualcomm.com/com	O-QUA-SDA6-271119/2419

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	pany/product-security/bulletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2420

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 /	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2421

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2422
Improper Restriction of Operations within the	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SDA6-271119/2423

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, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sdm439_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2424

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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2425
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2427
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	271119/2428
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2429

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2430
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	271119/2431
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2432

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2433
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2434

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2435
Improper Restriction	06-11-2019	10	Dereference on uninitialized buffer can happen when	https://source.android.	O-QUA-SDM4-271119/2436

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2437

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2438
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2439

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2440

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2441
Improper	06-11-2019	4.6	Arbitrary buffer write issue	https://sou	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	rce.android.com/security/bulletin/	271119/2442
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2443

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM4-271119/2444

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2445
Improper Validation of	06-11-2019	10	Out of boundary access due to token received from ADSP	https://source.android.	O-QUA-SDM4-271119/2446

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	com/security/bulletin/	
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2447

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SDM4-271119/2448

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2332**		
sdm630_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2449
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2450

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2451
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	271119/2452
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2453

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2454
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	271119/2455
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2456

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

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 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2457
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2458

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2459

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2460
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2461

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2462
Improper	06-11-2019	10	Improper validation of read	https://sou	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	rce.android.com/security/bulletin/	271119/2463
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2464

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2465

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2466
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2467

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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2468

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-SDM6-271119/2469

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2470
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2471

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2472

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2473
sdm660_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2474

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon 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-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2475

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10504		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2476
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2477

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2478

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2479
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2480

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2481
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	O-QUA-SDM6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/2482
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2483

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2484
Improper Restriction	06-11-2019	10	Dereference on uninitialized buffer can happen when	https://source.android.	O-QUA-SDM6-271119/2485

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2486

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2487
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2488

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2489

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2490
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2492

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

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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2493
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2494

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SDM6-271119/2495

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2496

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2497
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SDM6-271119/2499

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2332**		
snapdragon_high_med_2016_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2500

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2501
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2502

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2503
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2504

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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-2019-2285**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2505

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SNAP-271119/2506
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SNAP-271119/2507

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
mdm9150_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2509

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2510
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2511

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2512

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

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, SDX24 **CVE ID : CVE-2019-10529**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2513
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2514

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2515

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2516
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory	https://source.android.com/securit	O-QUA-MDM9-271119/2517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	y/bulletin/	
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MDM9-271119/2518

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2519

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2520
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2521

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2522

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2523
mdm9640_firmware					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2524
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2525

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2526

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2527
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2528

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2529
Out-of-	06-11-2019	7.5	Buffer over-read may occur	https://sou	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	rce.android.com/security/bulletin/	MDM9-271119/2530
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2531

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 710 / SD 670, SD 730, SD 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2532
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2533

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2534

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2535

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2536
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2537

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2538

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2539
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-MDM9-271119/2540

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
msm8909w_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2542
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2543

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2544
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2546

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

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, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2547
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2548

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2549

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2550
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2551

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2552
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2553

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2554

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2555
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2556

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2557
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2558

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2559

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2560
Improper Input	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence	https://source.android.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			header during HEVC or AVC encoding. 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-2019-10495**	com/security/bulletin/	271119/2561
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605,	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2562

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

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-MSM8-271119/2563

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2564
Improper Restriction of	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might	https://source.android.com/securit	O-QUA-MSM8-271119/2565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2566

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-MSM8-271119/2567
Improper Restriction	06-11-2019	10	Memory corruption while accessing the memory as	https://source.android.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	com/security/bulletin/	271119/2568
qcs605_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2569

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2570
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2571

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2572

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2573
Concurrent Execution using Shared Resource	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2574

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
with Improper Synchronization ('Race Condition')			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2575

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2576
Improper Restriction of Operations within the Bounds of a	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2577

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2578
Improper	06-11-2019	7.2	Thread start can cause	https://sou	O-QUA-QCS6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	rce.android.com/security/bulletin/	271119/2579
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2580

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2581
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2582

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2583

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2584
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2586

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

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2587

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-QCS6-271119/2588
N/A	06-11-2019	10	Lack of check to ensure	https://sou	O-QUA-QCS6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	rce.android.com/security/bulletin/	271119/2589
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2590

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

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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2591

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2331		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-QCS6-271119/2592
sd_670_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2593

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2594
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2595

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2596

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2597
Buffer Copy	06-11-2019	7.5	While playing the clip which	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	rce.android.com/security/bulletin/	271119/2598
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2599

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

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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2600
Improper	06-11-2019	10	Out of bound access due to	https://sou	O-QUA-SD_6-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	rce.android.com/security/bulletin/	271119/2601
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2602

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2603
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2604

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2605

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2606
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2607

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2608

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2610

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2611

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2612
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur	https://www.qualcomm.com/com	O-QUA-SD_6-271119/2613

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	pany/product-security/bulletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2614

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2615

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2616
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2617

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2618

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2332**		
sd_675_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2619
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2620

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2621

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2622
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2623

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2624

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2625
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2626

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2627
Improper	06-11-2019	10	Out of bound access due to	https://sou	O-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	rce.android.com/security/bulletin/	271119/2628
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2629

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2630
Improper Restriction of Operations within the	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2631

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2632

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2633
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2634

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2635

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2636
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2637

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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2638

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2639
Improper Restriction of	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might	https://source.android.com/securit	O-QUA-SD_6-271119/2640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2641

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_6-271119/2642
Improper Restriction	06-11-2019	10	Memory corruption while accessing the memory as	https://source.android.	O-QUA-SD_6-271119/2643

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	com/security/bulletin/	
sd_710_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2645
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2646

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2647

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2648
Buffer Copy without Checking Size of Input	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2649

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2650

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

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, SDX24 **CVE ID : CVE-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2651
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2652

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2653

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2654
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2655

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2656

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2657
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2658

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

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 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2659
NULL	06-11-2019	5	Null pointer dereference can	https://sou	O-QUA-SD_7-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	rce.android.com/security/bulletin/	271119/2660
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2661

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2662

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2663
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_7-271119/2664

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	lletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2665

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2666

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2324		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2667
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2668

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2669

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332**		
sd_712_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2670
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2672

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10505		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2673
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2674

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDX20 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2676
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2678

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2679
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2680

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2681
Improper Restriction	06-11-2019	7.2	Thread start can cause invalid memory writes to	https://source.android.	O-QUA-SD_7-271119/2682

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	com/security/bulletin/	
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2683

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2684
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2685

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2686

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2687
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC	https://source.android.com/securit	O-QUA-SD_7-271119/2688

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encoding. 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-2019-10495**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2689

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

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_7-271119/2690

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2691
Improper Restriction of Operations	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2692

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2693

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

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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_7-271119/2694
Improper Restriction of	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated	https://source.android.com/securit	O-QUA-SD_7-271119/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	y/bulletin/	
sd_820_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2696

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

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-2019-10496**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2697

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2698
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2699

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2700

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2701
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2702

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2703
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2704

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2705

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2706
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2707

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2708

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2283		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2709
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2710

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2711

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2712
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2713

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-271119/2714

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2715

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2716
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2717

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2718

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2719
sd_835_firmware					
Buffer Copy without Checking Size of Input	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer	https://source.android.com/securit	O-QUA-SD_8-271119/2720

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			overflow 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-2019-10496**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2721

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2722

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10512		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2723
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2724

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

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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2725
Use After	06-11-2019	7.5	Use after free issue in kernel	https://sou	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	rce.android.com/security/bulletin/	271119/2726
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2727

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

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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2728
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2729

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2730

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2731
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2732

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2733
Out-of-bounds	06-11-2019	10	Out of bound write issue is observed while giving	https://source.android.	O-QUA-SD_8-271119/2734

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			information about properties that have been set so far for playing video 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-2019-2285**	com/security/bulletin/	
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2735

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2736

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2737
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2738

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-271119/2739

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2740

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2741
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2742

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2743

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
sd_845_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2744
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2746
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2748

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2749
Buffer Copy without Checking Size of Input	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2750

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2751

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

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, SDX24 **CVE ID : CVE-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2752
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2753

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2754

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2755
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2756

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2757

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2758
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2759

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

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 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2760
NULL	06-11-2019	5	Null pointer dereference can	https://sou	O-QUA-SD_8-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer Dereference			occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	rce.android.com/security/bulletin/	271119/2761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2762

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2763

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2764
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_8-271119/2765

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	lletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2766

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2767

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2324		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2768
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2769

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2770

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332**		
sd_850_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2771
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2773
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2774

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2775

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2776
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2778

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2779
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2780

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2781

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2782
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2783

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2784

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2785
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2786

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

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 625, SD 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2787
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	O-QUA-SD_8-271119/2788

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2789

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2790

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2791
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are	https://www.qualcomm.com/company/product-security/bu	O-QUA-SD_8-271119/2792

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	lletins	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2793

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2794

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2324		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2795
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2796

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2797

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332**		
sd_855_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2798
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2799

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2800

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10505		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2801
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2803

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2804
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2805

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2806
Improper	06-11-2019	10	Out of bound access due to	https://sou	O-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	rce.android.com/security/bulletin/	271119/2807
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2808

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2809
Improper Restriction of Operations within the	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2810

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2811

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2812
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2813

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2814

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2815
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2816

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2817

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-271119/2818

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2275**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2819
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2820

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2821

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2822
Improper Restriction of Operations within the Bounds of a	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sdx20_firmware					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2824

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2825

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2826
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2827

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2828

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2829
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2830

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2831
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2832

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2833

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2834
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2835

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
			Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2836
Integer	06-11-2019	7.5	While processing vendor	https://sou	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	rce.android.com/security/bulletin/	271119/2837
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2838

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2839

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2840
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2841

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2842

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2843
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2844

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2845

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
sxr1130_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2846
Improper Validation of	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto,	https://source.android.com/securit	O-QUA-SXR1-271119/2847

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	y/bulletin/	
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206,	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2848

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2849
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2850

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2851

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2852
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	O-QUA-SXR1-271119/2853

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SXR1-271119/2854

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
sd_8cx_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2855

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2856
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2857

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2858

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2859
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	O-QUA-SD_8-271119/2860

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm	https://www.qualcomm.com/company/product-security/bulletins	O-QUA-SD_8-271119/2861

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

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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
sdx24_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2862
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2863

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2864

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2865
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2866

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2867

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2868
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2869

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2870
Improper Restriction of	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating	https://source.android.com/securit	O-QUA-SDX2-271119/2871

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			pointer can lead to out-of-bound access 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, 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 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-2019-2283**	y/bulletin/	
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2872

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2873

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2874
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2875

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2876
Integer Overflow or	06-11-2019	10	Possible Integer overflow because of subtracting two	https://source.android.	O-QUA-SDX2-271119/2877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	O-QUA-SDX2-271119/2878

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2332**		
Redhat					
enterprise_linux_desktop					
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensuse-security-announce/2019-10/msg00048.html	O-RED-ENTE-271119/2879

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**		
enterprise_linux_server					
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensuse-security-announce/2	O-RED-ENTE-271119/2880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**	019-10/msg00048.html	
enterprise_linux_workstation					
N/A	01-11-2019	5	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but	https://access.redhat.com/errata/RHSA-2019:2060, https://bugs.debian.org/cgi-	O-RED-ENTE-271119/2881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation. **CVE ID : CVE-2019-6470**	bin/bugreport.cgi?bug=896122, https://lists.opensuse.org/opensuse-security-announce/2019-10/msg00048.html	
enterprise_linux					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	08-11-2019	3.5	A flaw was found in the 'deref' plugin of 389-ds-base where it could use the 'search' permission to display attribute values. In some configurations, this could allow an authenticated attacker to view private attributes, such as password hashes. **CVE ID : CVE-2019-14824**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-14824	O-RED-ENTE-271119/2882
Samsung					
galaxy_s8_plus_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth, resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**	N/A	O-SAM-GALA-271119/2883

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**	N/A	O-SAM-GALA-271119/2884
galaxy_s3_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung	N/A	O-SAM-GALA-271119/2885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth, resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**		
Information Exposure	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over	N/A	O-SAM-GALA-271119/2886

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**		
galaxy_note_2_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth, resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**	N/A	O-SAM-GALA-271119/2887
Information Exposure	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor:	N/A	O-SAM-GALA-271119/2888

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**		
Technicolor					
tc7300.b0_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	3.5	An XSS vulnerability on Technicolor TC7300 STFA.51.20 devices allows remote attackers to inject arbitrary web script via the FileName parameter to /FTPDiag.asp. **CVE ID : CVE-2019-17523**	N/A	O-TEC-TC73-271119/2889
Improper Neutralization of Input	13-11-2019	3.5	An XSS vulnerability on Technicolor TC7300 STFA.51.20 devices allows	N/A	O-TEC-TC73-271119/2890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			remote attackers to inject arbitrary web script via the "Connected Clients" field to /wlanAccess.asp. An intranet host can use a crafted hostname to exploit this. **CVE ID : CVE-2019-17524**		
western_digital					
my_cloud_ex2_ultra_firmware					
Out-of-bounds Write	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.183 allows web users (including guest accounts) to remotely execute arbitrary code via a download_mgr.cgi stack-based buffer overflow. **CVE ID : CVE-2019-18929**	N/A	O-WES-MY_C-271119/2891
Out-of-bounds Write	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.183 allows web users (including guest account) to remotely execute arbitrary code via a stack-based buffer overflow. There is no size verification logic in one of functions in libscheddl.so, and download_mgr.cgi makes it possible to enter large-sized f_idx inputs. **CVE ID : CVE-2019-18930**	N/A	O-WES-MY_C-271119/2892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.195 allows a Buffer Overflow with Extended Instruction Pointer (EIP) control via crafted GET/POST parameters. **CVE ID : CVE-2019-18931**	N/A	O-WES-MY_C-271119/2893

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ZTE					
mf910s_firmware					
Information Exposure	07-11-2019	1.9	The Sec Consult Security Lab reported an information disclosure vulnerability in MF910S product to ZTE PSIRT in October 2019. Through the analysis of related product team, the information disclosure vulnerability is confirmed. The MF910S product's one-click upgrade tool can obtain the Telnet remote login password in the reverse way. If Telnet is opened, the attacker can remotely log in to the device through the cracked password, resulting in information leakage. The MF910S was end of service on October 23, 2019, ZTE recommends users to choose new products for the purpose of better security. **CVE ID : CVE-2019-3422**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011722	O-ZTE-MF91-271119/2894
zxupn-9000e_firmware					
Incorrect Default Permissions	08-11-2019	7.5	The 9000EV5.0R1B12 version, and all earlier versions of ZTE product ZXUPN-9000E are impacted by vulnerability of permission and access control. An attacker could exploit this vulnerability to directly reset or change passwords of other accounts. **CVE ID : CVE-2019-3425**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011683	O-ZTE-ZXUP-271119/2895
Improper	08-11-2019	7.5	The 9000EV5.0R1B12	http://supp	O-ZTE-ZXUP-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			version, and all earlier versions of ZTE product ZXUPN-9000E are impacted by the input validation vulnerability. An attacker could exploit this vulnerability for unauthorized operations. **CVE ID : CVE-2019-3426**	ort.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011683	271119/2896
Zyxel					
2.00\(abbx.3\)					
Incorrect Authorization	12-11-2019	4	ZyXEL P-1302-T10D v3 devices with firmware version 2.00(ABBX.3) and earlier do not properly enforce access control and could allow an unauthorized user to access certain pages that require admin privileges. **CVE ID : CVE-2019-15815**	https://www.zyxel.com/support/P1302-T10D-v3-modem-insecure-direct-object-reference-vulnerability.shtml	O-ZYX-2.00-271119/2897
Hardware					
archos					
safe-t					
Information Exposure	02-11-2019	1.9	On Archos Safe-T devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets	N/A	H-ARC-SAFE-271119/2898

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			such as the PIN and BIP39 mnemonic. In other words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data. **CVE ID : CVE-2019-14358**		
Cisco					
mds_9100					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-MDS_-271119/2899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
mds_9200					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-MDS_-271119/2900

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
mds_9500					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-MDS_-271119/2901
mds_9700					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-MDS_-271119/2902

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_31128pq					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2903

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3132c-z					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2904

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3132q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2905

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3132q-v					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2906
nexus_3132q-xl					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2907

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3164q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2908

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3172					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2909

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3172pq-xl					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2910

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3172tq					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2911
nexus_3172tq-32t					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2912

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3172tq-xl					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3232c					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2914

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3264c-e					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2915

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3264q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2916
nexus_3408-s					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2917

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_34180yc					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3432d-s					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2919

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3464c					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2920

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3524					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2921
nexus_3524-x					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2922

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3524-xl					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3548					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2924

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3548-x					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2925

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3548-xl					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2926
nexus_5548p					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2927

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5548up					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2928

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5596t					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2929

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5596up					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2930

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_56128p					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2931
nexus_5624q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2932

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5648q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2933

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5672up					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2934

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_5696q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2935

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_36180yc-r					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2936
nexus_3636c-r					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2937

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_7000					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2938

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_7700					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2939

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_4115					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-FIRE-271119/2940

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
firepower_4125					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-FIRE-271119/2941
firepower_4145					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-FIRE-271119/2942

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_4110					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-FIRE-271119/2943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_4120					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-FIRE-271119/2944

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_4140					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-FIRE-271119/2945

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
firepower_4150					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-FIRE-271119/2946
ucs_6200					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-UCS_-271119/2947

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
ucs_6300					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-UCS_-271119/2948

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_9300_sm-24					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-FIRE-271119/2949

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_9300_sm-36					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-FIRE-271119/2950

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
firepower_9300_sm-40					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-FIRE-271119/2951
firepower_9300_sm-44					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-FIRE-271119/2952

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_9300_sm-44_x_3					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-FIRE-271119/2953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_9300_sm-48					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-FIRE-271119/2954

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
firepower_9300_sm-56					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-FIRE-271119/2955

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
firepower_9300_sm-56_x_3					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-FIRE-271119/2956
nexus_9000v					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2957

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_92160yc-x					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2958

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_92300yc					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2959

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_92304qc					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2960

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_92348gc-x					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2961
nexus_9236c					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2962

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9272q					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2963

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93108tc-ex					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2964

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93108tc-fx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2965

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_93120tx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2966
nexus_93128tx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2967

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93180lc-ex					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93180yc-ex					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2969

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93180yc-fx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2970

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_93216tc-fx2					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2971
nexus_93240yc-fx2					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2972

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9332c					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2973

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9332pq					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2974

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_93360yc-fx2					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2975

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_9336c-fx2					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2976
nexus_9336pq_aci_spine					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2977

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9348gc-fxp					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9364c					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2979

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9372px					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2980

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_9372px-e					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2981
nexus_9372tx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2982

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9372tx-e					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2983

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9396px					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2984

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9396tx					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2985

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_9504					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2986
nexus_9508					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2987

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_9516					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3016					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2989

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_3048					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability.	N/A	H-CIS-NEXU-271119/2990

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-1734		
nexus_3064					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**	N/A	H-CIS-NEXU-271119/2991
nexus_3064-t					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker	N/A	H-CIS-NEXU-271119/2992

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_31108pc-v					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC)	N/A	H-CIS-NEXU-271119/2993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
nexus_31108tc-v					
Information Exposure	05-11-2019	2.1	A vulnerability in the implementation of a CLI diagnostic command in Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to view sensitive system files that should be restricted. The attacker could use this information to conduct additional reconnaissance attacks. The vulnerability is due to incomplete role-based access control (RBAC) verification. An attacker could exploit this vulnerability by authenticating to the device and issuing a specific CLI diagnostic command with crafted user-input parameters. An exploit could	N/A	H-CIS-NEXU-271119/2994

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to perform an arbitrary read of a file on the device, and the file may contain sensitive information. The attacker needs valid device credentials to exploit this vulnerability. **CVE ID : CVE-2019-1734**		
Dlink					
dir-600_b1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	H-DLI-DIR--271119/2995
dir-615_j1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00.	N/A	H-DLI-DIR--271119/2996

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-18852		
dir-645_a1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	H-DLI-DIR--271119/2997
dir-815_a1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	H-DLI-DIR--271119/2998
dir-823_a1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1	N/A	H-DLI-DIR--271119/2999

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**		
dir-842_c1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	H-DLI-DIR--271119/3000
dir-890l_a1					
Use of Hard-coded Credentials	11-11-2019	10	Certain D-Link devices have a hardcoded Alphanetworks user account with TELNET access because of /etc/config/image_sign or /etc/alpha_config/image_sign. This affects DIR-600 B1 V2.01 for WW, DIR-890L A1 v1.03, DIR-615 J1 v100 (for DCN), DIR-645 A1 v1.03, DIR-815 A1 v1.01, DIR-823 A1 v1.01, and DIR-842 C1 v3.00. **CVE ID : CVE-2019-18852**	N/A	H-DLI-DIR--271119/3001
fastweb					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fastgate					
Information Exposure	02-11-2019	5	Fastweb FASTGate 1.0.1b devices allow partial authentication bypass by changing a certain check_pwd return value from 0 to 1. An attack does not achieve administrative control of a device; however, the attacker can view all of the web pages of the administration console. **CVE ID : CVE-2019-18661**	N/A	H-FAS-FAST-271119/3002
HP					
prodesk_490_g2_mt					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3003
prodesk_490_g3_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which	https://support.hp.com/rs-en/docume	H-HP-PROD-271119/3004

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	nt/c06456250	
prodesk_498_g2_mt					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3005
prodesk_498_g3_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP	https://support.hp.com/rs-	H-HP-PROD-271119/3006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	en/document/c06456250	
prodesk_600_g2_dm					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3007
prodesk_600_g2_sff					
Improper Input	05-11-2019	9	A potential security vulnerability has been	https://support.hp.com	H-HP-PROD-271119/3008

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	/rs-en/document/c06456250	
proone_400_g2_aio					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROO-271119/3009
proone_600_g2_aio					
Improper	05-11-2019	9	A potential security	https://sup	H-HP-PROO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	port.hp.com/rs-en/document/c06456250	271119/3010
rp2_retail_system					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-RP2_-271119/3011
rp9_g1_retail_system_9015					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-RP9_-271119/3012
rp9_g1_retail_system_9018					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-RP9_-271119/3013

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
zbook_14_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3014
zbook_14					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3015

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-16284		
zbook_15_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3016
zbook_15_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3017

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_15					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3018
zbook_15u_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3019

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_15u_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3020
zbook_17_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_17_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3022
zbook_17					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3023

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
zbook_studio_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ZBOO-271119/3024
z1_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	H-HP-Z1_G-271119/3025

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
z2_mini_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-Z2_M-271119/3026
z238_microtower					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	H-HP-Z238-271119/3027

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
z240_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-Z240-271119/3028
z240_tower					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	H-HP-Z240-271119/3029

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
sprout_pro					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-SPRO-271119/3030
pro_tablet_610_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be	https://support.hp.com/rs-en/document/c06456250	H-HP-PRO_-271119/3031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
pro_x2_612_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PRO_-271119/3032
probook_11_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_11_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3034
probook_430_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_430_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3036
probook_430_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3037

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_440_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3038
probook_440_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3039

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
probook_440_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3040
probook_450_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution	https://support.hp.com/rs-en/document/c064562	H-HP-PROB-271119/3041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	50	
probook_450_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3042
probook_450_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which	https://support.hp.com/rs-en/docume	H-HP-PROB-271119/3043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	nt/c06456250	
probook_470_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3044
probook_470_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP	https://support.hp.com/rs-	H-HP-PROB-271119/3045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	en/document/c06456250	
probook_470_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3046
probook_640_g1					
Improper Input	05-11-2019	9	A potential security vulnerability has been	https://support.hp.com	H-HP-PROB-271119/3047

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	/rs-en/document/c06456250	
probook_640_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3048
probook_650_g1					
Improper	05-11-2019	9	A potential security	https://sup	H-HP-PROB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	port.hp.com/rs-en/document/c06456250	271119/3049
probook_650_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3050
probook_x360_11_g1					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROB-271119/3051
prodesk_400_g1_dm					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3052

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
prodesk_400_g2_dm					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3053
prodesk_400_g2.5_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3054

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-16284		
prodesk_400_g3_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3055
prodesk_405_g2_mt					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3056

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
prodesk_485_g2_mt					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3057
prodesk_480_g3_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	H-HP-PROD-271119/3058

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_820_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3059
elitebook_820_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_820_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3061
elitebook_828_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3062

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_840_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3063
elitebook_840_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_840_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3065
elitebook_848_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3066

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_850_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3067
elitebook_850_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3068

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_850_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3069
elitebook_folio_1020_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3070

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_folio_1040_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3071
elitebook_folio_1040_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3072

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_folio_9480m					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3073
elitebook_folio_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_revolve_810_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3075
elitebook_revolve_810_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3076

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitedesk_800_g2_dm					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3077
elitedesk_800_g2_sff					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3078

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitedesk_800_g2_twr					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3079
eliteone_800_g2_aio					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution	https://support.hp.com/rs-en/document/c064562	H-HP-ELIT-271119/3080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	50	
elitepad_1000_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3081
mp9_g2_retail_system					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which	https://support.hp.com/rs-en/docume	H-HP-MP9_-271119/3082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	nt/c06456250	
pro_tablet_10_ee_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-PRO_-271119/3083
pro_tablet_608_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP	https://support.hp.com/rs-	H-HP-PRO_-271119/3084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	en/document/c06456250	
k9z74d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-K9Z7-271119/3085
d3q21a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3086
d3q21b					
Reachable	07-11-2019	3.3	For the printers listed a	N/A	H-HP-D3Q2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Assertion			maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		271119/3087
d3q21c					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3088
d3q21d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3089
k9z76a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-K9Z7-271119/3090

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
k9z76b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-K9Z7-271119/3091
k9z76d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-K9Z7-271119/3092
260_g1_dm					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250.	https://support.hp.com/rs-en/document/c06456250	H-HP-260_-271119/3093

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-16284		
280_pro_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-280_-271119/3094
285_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-	https://support.hp.com/rs-en/document/c06456250	H-HP-285_-271119/3095

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			en/document/c06456250. **CVE ID : CVE-2019-16284**		
340_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-340_-271119/3096
340_g4					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in	https://support.hp.com/rs-en/document/c06456250	H-HP-340_-271119/3097

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
346_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-346_-271119/3098
346_g4					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are	https://support.hp.com/rs-en/document/c06456250	H-HP-346_-271119/3099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
348_g3					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-348_-271119/3100
348_g4					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected	https://support.hp.com/rs-en/document/c06456250	H-HP-348_-271119/3101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elite_slice					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3102
elite_x2_1011_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode)	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elite_x2_1012_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3104
elitebook_1030_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_1040_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3106
elitebook_720_g1_					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3107

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_720_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3108
elitebook_740_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3109

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_740_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3110
elitebook_750_g1					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3111

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**		
elitebook_750_g2					
Improper Input Validation	05-11-2019	9	A potential security vulnerability has been identified in multiple HP products and versions which involves possible execution of arbitrary code during boot services that can result in elevation of privilege. The EFI_BOOT_SERVICES structure might be overwritten by an attacker to execute arbitrary SMM (System Management Mode) code. A list of affected products and versions are available in https://support.hp.com/rs-en/document/c06456250. **CVE ID : CVE-2019-16284**	https://support.hp.com/rs-en/document/c06456250	H-HP-ELIT-271119/3112
d9l63a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device.	N/A	H-HP-D9L6-271119/3113

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6337		
d9l64a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D9L6-271119/3114
t0g70a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-T0G7-271119/3115
j3p65a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J3P6-271119/3116
j3p68a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer	N/A	H-HP-J3P6-271119/3117

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
j6u57a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J6U5-271119/3118
j6u57b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J6U5-271119/3119
j9v80a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J9V8-271119/3120
j9v80b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP	N/A	H-HP-J9V8-271119/3121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
j6u55a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J6U5-271119/3122
j6u55d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J6U5-271119/3123
j6u51b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J6U5-271119/3124
j9v82a					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J9V8-271119/3125
j9v82d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J9V8-271119/3126
j9v78b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-J9V7-271119/3127
d3q15a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device.	N/A	H-HP-D3Q1-271119/3128

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6337		
d3q15b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3129
d3q15d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3130
d3q16a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3131
d3q16d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer	N/A	H-HP-D3Q1-271119/3132

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
w2z52b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-W2Z5-271119/3133
d3q19a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3134
d3q19b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3135
d3q19d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP	N/A	H-HP-D3Q1-271119/3136

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**		
d3q20a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3137
d3q20b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3138
d3q20c					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3139
d3q20d					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q2-271119/3140
w2z53b					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-W2Z5-271119/3141
2dr21d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-2DR2-271119/3142
d3q17a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device.	N/A	H-HP-D3Q1-271119/3143

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6337		
d3q17d					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-D3Q1-271119/3144
k9z74a					
Reachable Assertion	07-11-2019	3.3	For the printers listed a maliciously crafted print file might cause certain HP Inkjet printers to assert. Under certain circumstances, the printer produces a core dump to a local device. **CVE ID : CVE-2019-6337**	N/A	H-HP-K9Z7-271119/3145
hpe					
nimble_storage_af20_all_flash_array					
Improper Privilege Management	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older,	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3146

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**		
nimble_storage_af20q_all_flash_dual_controller					
Improper Privilege Management	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3147
nimble_storage_af40_all_flash_dual_controller					
Improper Privilege	07-11-2019	10	Potential security vulnerabilities have been	https://support.hpe.co	H-HPE-NIMB-271119/3148

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	m/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	
nimble_storage_af60_all_flash_dual_controller					
Improper Privilege Management	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**		
nimble_storage_af80_all_flash_dual_controller					
Improper Privilege Managemen t	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3150
nimble_storage_cs3000					
Improper Privilege Managemen	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble	https://support.hpe.com/hpsc/do	H-HPE-NIMB-271119/3151

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	c/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	
nimble_storage_cs5000					
Improper Privilege Management	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays -	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3152

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**		
nimble_storage_cs7000					
Improper Privilege Managemen t	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03964en_us	H-HPE-NIMB-271119/3153
nimble_storage_secondary_flash_arrays					
Improper Privilege Managemen t	07-11-2019	10	Potential security vulnerabilities have been identified with HPE Nimble Storage systems in multi	https://support.hpe.com/hpsc/doc/public/di	H-HPE-NIMB-271119/3154

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			array group configurations. The vulnerabilities could be remotely exploited by an attacker to gain elevated privileges or disclose information the array. Affected products and versions include: Nimble Storage Hybrid Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage All Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older Nimble Storage Secondary Flash Arrays - 5.1.2.0 and older, 5.0.7.0 and older, 4.5.4.0 and older, and 3.9.1.0 and older **CVE ID : CVE-2019-11996**	splay?docLocale=en_US&docId=emr_na-hpesbst03964en_us	
Huawei					
honor_v20					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20 smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system does not lock certain function properly, when the function is called by multiple processes could cause out of	N/A	H-HUA-HONO-271119/3155

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**		
p20_pro					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**	N/A	H-HUA-P20_-271119/3156
mate_rs					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A	N/A	H-HUA-MATE-271119/3157

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**		
taurus-al00b					
Improper Authentication	13-11-2019	6.8	Huawei smartphones with versions earlier than Taurus-AL00B 10.0.0.41(SP2C00E41R3P2) have an improper authentication vulnerability. Successful exploitation may cause the attacker to access specific components. **CVE ID : CVE-2019-5233**	N/A	H-HUA-TAUR-271119/3158
elle-al00b					
Insufficient Verification of Data Authenticity	13-11-2019	4.6	Smartphones with software of ELLE-AL00B 9.1.0.109(C00E106R1P21), 9.1.0.113(C00E110R1P21), 9.1.0.125(C00E120R1P21), 9.1.0.135(C00E130R1P21), 9.1.0.153(C00E150R1P21), 9.1.0.155(C00E150R1P21), 9.1.0.162(C00E160R2P1)	N/A	H-HUA-ELLE-271119/3159

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an insufficient verification vulnerability. The system does not verify certain parameters sufficiently, an attacker should connect to the phone and gain high privilege to launch the attack. Successful exploit could cause DOS or malicious code execution. **CVE ID : CVE-2019-5246**		
emily-al00a					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**	N/A	H-HUA-EMIL-271119/3160

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
emily-tl00b					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**	N/A	H-HUA-EMIL-271119/3161
emily-l09c					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11),	N/A	H-HUA-EMIL-271119/3162

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
hima-l09ca					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice.	N/A	H-HUA-HIMA-271119/3163

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
hima-l29ca					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**	N/A	H-HUA-HIMA-271119/3164
hima-l29c					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-	N/A	H-HUA-HIMA-271119/3165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution. **CVE ID : CVE-2019-5282**		
honor_10_lite					
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before 9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**	N/A	H-HUA-HONO-271119/3166

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
honor_8a					
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before 9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**	N/A	H-HUA-HONO-271119/3167
huawei_y6					
Information Exposure	13-11-2019	2.1	Honor 10 Lite, Honor 8A, Huawei Y6 mobile phones with the versions before 9.1.0.217(C00E215R3P1), the versions before 9.1.0.205(C00E97R1P9), the versions before 9.1.0.205(C00E97R2P2) have an information leak vulnerability. Due to improper function error records of some module, an attacker with the access permission may exploit the vulnerability to obtain some information. **CVE ID : CVE-2019-5292**	N/A	H-HUA-HUAW-271119/3168
ar120-s					
Missing Release of	13-11-2019	4	Some Huawei products have a memory leak vulnerability	N/A	H-HUA-AR12-271119/3169

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource after Effective Lifetime			when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**		
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR12-271119/3170
ar1200					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR12-271119/3171
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote,	N/A	H-HUA-AR12-271119/3172

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**		
ar1200-s					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR12-271119/3173
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR12-271119/3174
p30_pro					
Concurrent Execution	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20	N/A	H-HUA-P30_-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
using Shared Resource with Improper Synchronization ('Race Condition')			smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system does not lock certain function properly, when the function is called by multiple processes could cause out of bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**		271119/3175
p30					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	12-11-2019	6.8	Certain detection module of P30, P30 Pro, Honor V20 smartphone whith Versions earlier than ELLE-AL00B 9.1.0.193(C00E190R1P21), Versions earlier than VOGUE-AL00A 9.1.0.193(C00E190R1P12), Versions earlier than Princeton-AL10B 9.1.0.233(C00E233R4P3) have a race condition vulnerability. The system does not lock certain function properly, when the function is called by multiple processes could cause out of	N/A	H-HUA-P30-271119/3176

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bound write. An attacker tricks the user into installing a malicious application, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5228**		
Insufficient Verification of Data Authenticity	12-11-2019	4.6	P30 smartphones with versions earlier than ELLE-AL00B 9.1.0.193(C00E190R2P1) have an insufficient verification vulnerability. The system does not verify certain parameters sufficiently, an attacker should connect to the phone and gain high privilege to launch the attack, successful exploit could cause malicious code execution. **CVE ID : CVE-2019-5229**	N/A	H-HUA-P30-271119/3177
Incorrect Authorizatio n	13-11-2019	2.1	P30 smartphones with versions earlier than ELLE-AL00B 9.1.0.186(C00E180R2P1) have an improper authorization vulnerability. The software incorrectly performs an authorization check when a user attempts to perform certain action. Successful exploit could allow the attacker to update a crafted package. **CVE ID : CVE-2019-5231**	N/A	H-HUA-P30-271119/3178
honor_play					
Improper Authenticati	12-11-2019	1.9	Honor play smartphones with versions earlier than	N/A	H-HUA-HONO-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			Cornell-AL00A 9.1.0.321(C00E320R1P1T8) have an insufficient authentication vulnerability. The system has a logic judge error under certain scenario. Successful exploit could allow the attacker to modify the alarm clock settings after a serious of uncommon operations without unlock the screen lock. **CVE ID : CVE-2019-5213**		271119/3179
emily-l29c					
Double Free	13-11-2019	6.8	Bastet module of some Huawei smartphones with Versions earlier than Emily-AL00A 9.0.0.182(C00E82R1P21), Versions earlier than Emily-TL00B 9.0.0.182(C01E82R1P21), Versions earlier than Emily-L09C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.203(C432E7R1P11), Versions earlier than Emily-L29C 9.0.0.202(C185E2R1P12) have a double free vulnerability. An attacker tricks the user into installing a malicious application, which frees on the same memory address twice. Successful exploit could result in malicious code execution.	N/A	H-HUA-EMIL-271119/3180

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-5282		
p20					
Improper Input Validation	13-11-2019	4.3	P20 Pro, P20, Mate RS smartphones with versions earlier than Charlotte-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than Emily-AL00A 9.1.0.321(C00E320R1P1T8), versions earlier than NEO-AL00D NEO-AL00 9.1.0.321(C786E320R1P1T8) have an improper validation vulnerability. The system does not perform a properly validation of certain input models, an attacker could trick the user to install a malicious application then craft a malformed model, successful exploit could allow the attacker to get and tamper certain output data information. **CVE ID : CVE-2019-5230**	N/A	H-HUA-P20-271119/3181
ar150					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR15-271119/3182

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR15-271119/3183
ar150-s					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR15-271119/3184
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR15-271119/3185

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ar160					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR16-271119/3186
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR16-271119/3187
ar200					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR20-271119/3188

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR20-271119/3189
ar200-s					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR20-271119/3190
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR20-271119/3191

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ar2200					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR22-271119/3192
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR22-271119/3193
ar2200-s					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR22-271119/3194

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR22-271119/3195
ar3200					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR32-271119/3196
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR32-271119/3197

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ar3600					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-AR36-271119/3198
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-AR36-271119/3199
netengine16ex					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-NETE-271119/3200

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-NETE-271119/3201
srg1300					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-SRG1-271119/3202
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-SRG1-271119/3203

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
srg2300					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-SRG2-271119/3204
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-SRG2-271119/3205
srg3300					
Missing Release of Resource after Effective Lifetime	13-11-2019	4	Some Huawei products have a memory leak vulnerability when handling some messages. A remote attacker with operation privilege could exploit the vulnerability by sending specific messages continuously. Successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5293**	N/A	H-HUA-SRG3-271119/3206

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	13-11-2019	5	There is an out of bound read vulnerability in some Huawei products. A remote, unauthenticated attacker may send a corrupt or crafted message to the affected products. Due to a buffer read overflow error when parsing the message, successful exploit may cause some service to be abnormal. **CVE ID : CVE-2019-5294**	N/A	H-HUA-SRG3-271119/3207
Hyundaiusa					
hk-1000					
Information Exposure	02-11-2019	1.9	On Hyundai Pay Kasse HK-1000 devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. In other words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other	N/A	H-HYU-HK-1-271119/3208

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			circumstances, such as a stolen device that is not currently displaying secret data. **CVE ID : CVE-2019-14360**		
intelbras					
wrn_150					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-11-2019	4.3	An issue was discovered on Intelbras WRN 150 1.0.17 devices. There is stored XSS in the Service Name tab of the WAN configuration screen, leading to a denial of service (inability to change the configuration). **CVE ID : CVE-2019-17222**	N/A	H-INT-WRN_-271119/3209
Lenovo					
ideacentre_720-18icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3210
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3211
legion_c530-19icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain	N/A	H-LEN-LEGI-271119/3212

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3213
legion_c730-19ico					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3214
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3215
legion_t530-28icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3216
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3217

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_t730-28ico					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3218
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3219
h50-30g_desktop					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-H50--271119/3220
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-H50--271119/3221
m4500					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-M450-271119/3222
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-M450-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3223
m4500_id					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-M450-271119/3224
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-M450-271119/3225
m4550_id					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-M455-271119/3226
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-M455-271119/3227
qitian_4500					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-QITI-271119/3228

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3229
qitian_b4550					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3230
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3231
qitian_b4650					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3232
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-QITI-271119/3233

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
qitian_m4550					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3234
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3235
qitian_m4600					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3236
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3237
qitian_m4650					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3238

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3239
qt_m410					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QT_M-271119/3240
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QT_M-271119/3241
qt_b415					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QT_B-271119/3242
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QT_B-271119/3243
qt_m415					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-QT_M-271119/3244

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QT_M-271119/3245
thinkcentre_e73s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3246
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3247
thinkcentre_e74					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3248
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_e74s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3250
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3251
thinkcentre_e75t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3252
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3253
thinkcentre_e75s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3254

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3255
thinkcentre_m4500k					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3256
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3257
thinkcentre_m4500q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3258
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3259
thinkcentre_m4500t					

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3260
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3261
thinkcentre_m4500s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3262
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3263
thinkcentre_m4600t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3264
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3265

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m4600s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3266
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3267
thinkcentre_m610					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3268
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3269
thinkcentre_m6500t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3271
thinkcentre_m6500s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3272
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3273
thinkcentre_m6600					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3274
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3275

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkcentre_m6600q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3276
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3277
thinkcentre_m6600t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3278
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3279
thinkcentre_m6600s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3280
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-THIN-

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3281
thinkcentre_m700q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3282
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3283
thinkcentre_m700t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3284
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3285
thinkcentre_m700s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-THIN-271119/3286

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3287
thinkcentre_m710e					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3288
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3289
thinkcentre_m710q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3290
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-THIN-271119/3291

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkcentre_m710t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3292
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3293
thinkcentre_m710s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3294
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3295
thinkcentre_m720q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3296

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3297
thinkcentre_m720t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3298
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3299
thinkcentre_m720s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3300
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3301
thinkcentre_m73_tiny					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3302

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3303
thinkcentre_m73p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3304
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3305
thinkcentre_m800					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3306
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m8500t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3308
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3309
thinkcentre_m8500s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3310
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3311
thinkcentre_m8600t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3312

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3313
thinkcentre_m8600s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3314
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3315
thinkcentre_m900					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3316
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3317
thinkcentre_m910t					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3318
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3319
thinkcentre_m910s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3320
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3321
thinkcentre_m910q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3322
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m910x					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3324
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3325
thinkcentre_m920q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3326
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3327
thinkcentre_m920x					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3329
zhaoyang_e43-80_kbl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-ZHAO-271119/3330
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-ZHAO-271119/3331
xiaoxin_air-14iwl_2019					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3332
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3333

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
xiaoxin_air-15iwl_2019					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3334
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3335
xiaoxin-14_2019iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3336
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3337
xiaoxin-14iwl_qc_2019					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3338
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-XIAO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3339
xiaoxin-15_2019iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3340
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3341
xx_chao5000-ikbra					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XX_C-271119/3342
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XX_C-271119/3343
y7000_2019_1050					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-Y700-271119/3344

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-Y700-271119/3345
yoga_520-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3346
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3347
yoga_730-13iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3348
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-YOGA-271119/3349

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
yoga_730-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3350
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3351
yoga_s730-13iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3352
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3353
yoga_s940-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3354

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3355
yoga530-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3356
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3357
flex_6-1470					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-FLEX-271119/3358
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-FLEX-271119/3359
zhaoyang_k42-80					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-ZHAO-271119/3360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-ZHAO-271119/3361
xiaoxin_tide_7000-15_u22					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3362
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3363
xiaoxin_tide_7000-15_u42					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3364
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-XIAO-271119/3365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
zhaoyang_e53-80					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-ZHAO-271119/3366
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-ZHAO-271119/3367
l340-15irh					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-L340-271119/3368
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-L340-271119/3369
l340-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-L340-271119/3370

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-L340-271119/3371
l340-17irh					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-L340-271119/3372
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-L340-271119/3373
l340-15iwltouch					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-L340-271119/3374
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-L340-271119/3375
l340-17iwl					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-L340-271119/3376
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-L340-271119/3377
legion_y530-15ich					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3378
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3379
legion_y730-15ich					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3380
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-LEGI-271119/3381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
legion_y7000p-1060					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3382
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3383
legion_y530-15ich\(1060\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3384
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3385
legion_y730-17ich					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-LEGI-271119/3386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3387
legion_y740-15irhg					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3388
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3389
legion_y740-15ichg					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3390
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3391

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_y9000k_2019					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3392
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3393
legion_y740-17ichg					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3394
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3395
legion_y740-17irhg					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3396
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-LEGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3397
legion_y9000p_2019					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3398
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3399
lenovo_v720-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LENO-271119/3400
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LENO-271119/3401
legion_y520t_z370					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-LEGI-271119/3402

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3403
aio520-22ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3404
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO5-271119/3405
aio520-22iku					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3406
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-AIO5-271119/3407

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
aio520-24ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3408
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO5-271119/3409
aio520-24iku					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3410
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO5-271119/3411
aio520-27ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3412

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO5-271119/3413
thinkcentre_m700z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3414
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3415
thinkcentre_m800z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3416
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3417
thinkcentre_m810z					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3418

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3419
thinkcentre_m818z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3420
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3421
thinkcentre_m900z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3422
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m910z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3424
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3425
v410z\(yt_s4250\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V410-271119/3426
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V410-271119/3427
330-14ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-330--271119/3428

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3429
330-15ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3430
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3431
330-15ikbr_touch					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3432
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3433
330-17ikbr					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3434
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3435
720s_touch-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-720S-271119/3436
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-720S-271119/3437
720s-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-720S-271119/3438
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-720S-271119/3439

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
flex_5-1570\(r\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-FLEX-271119/3440
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-FLEX-271119/3441
k43c-80					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-K43C-271119/3442
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-K43C-271119/3443
v330-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-V330-271119/3444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V330-271119/3445
v330-14isk					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V330-271119/3446
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V330-271119/3447
v330-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V330-271119/3448
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V330-271119/3449

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
v330-15isk					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V330-271119/3450
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V330-271119/3451
v730-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V730-271119/3452
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V730-271119/3453
yoga_730-13ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3454
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-YOGA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3455
yoga_730-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3456
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3457
thinkpad_11e					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3458
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3459
miix_720-12ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-MIIX-271119/3460

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-MIIX-271119/3461
rescuer_y7000p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-RESC-271119/3462
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-RESC-271119/3463
rescuer_y7000p\(1060\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-RESC-271119/3464
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-RESC-271119/3465

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
rescuer_y7000					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-RESC-271119/3466
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-RESC-271119/3467
rescuer_y7000\(1060\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-RESC-271119/3468
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-RESC-271119/3469
s145-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S145-271119/3470

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S145-271119/3471
s145-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S145-271119/3472
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S145-271119/3473
s145-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S145-271119/3474
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S145-271119/3475
s145-15iwl					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-S145-271119/3476

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S145-271119/3477
340c-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-340C-271119/3478
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-340C-271119/3479
s340-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S340-271119/3480
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-S340-271119/3481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
s340-14iwl_touch					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S340-271119/3482
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S340-271119/3483
s340-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S340-271119/3484
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S340-271119/3485
s340-15iwl_touch					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-S340-271119/3486

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S340-271119/3487
s530-13iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S530-271119/3488
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S530-271119/3489
s540-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S540-271119/3490
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S540-271119/3491
s540-14iwl_touch					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S540-271119/3492
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S540-271119/3493
s540-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S540-271119/3494
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-S540-271119/3495
s940-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-S940-271119/3496
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-S940-271119/3497

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
v110-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V110-271119/3498
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V110-271119/3499
v110-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V110-271119/3500
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V110-271119/3501
v130-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-V130-271119/3502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V130-271119/3503
v130-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V130-271119/3504
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V130-271119/3505
v310-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V310-271119/3506
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V310-271119/3507

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
v310-14isk					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V310-271119/3508
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V310-271119/3509
v310-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V310-271119/3510
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V310-271119/3511
v310-15isk					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V310-271119/3512
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-V310-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3513
v320-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V320-271119/3514
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V320-271119/3515
v320-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V320-271119/3516
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V320-271119/3517
v320-17ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-V320-271119/3518

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V320-271119/3519
v510-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V510-271119/3520
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V510-271119/3521
v510-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V510-271119/3522
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-V510-271119/3523

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
wei5-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-WEI5-271119/3524
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-WEI5-271119/3525
wei5-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-WEI5-271119/3526
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-WEI5-271119/3527
xiaoxin_air_13iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3528

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3529
xiaoxin_air_14ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3530
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3531
xiaoxin_air_14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3532
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3533
xiaoxin_air_15ikbr					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-XIAO-271119/3534

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3535
xiaoxin_air_15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-XIAO-271119/3536
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-XIAO-271119/3537
thinkpad_10					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3538
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
yoga_11e_3rd_gen					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3540
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3541
yoga_11e_4th_gen					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YOGA-271119/3542
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGA-271119/3543
thinkpad_e450					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3544

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3545
thinkpad_e450c					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3546
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3547
thinkpad_e550					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3548
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3549
thinkpad_e550c					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3550
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3551
thinkpad_e490s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3552
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3553
thinkpad_s3					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3554
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3555

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m920t					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3556
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3557
thinkpad_13					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3558
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3559
thinkcentre_m920s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3561
thinkcentre_m93					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3562
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3563
thinkpad_e460					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3564
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3565

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_e560					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3566
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3567
thinkcentre_s510					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3568
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3569
v520s-08ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V520-271119/3570
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-V520-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3571
v520t-15ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V520-271119/3572
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V520-271119/3573
yangtian_afh110					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3574
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3575
yangtian_afh81					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-YANG-271119/3576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3577
thinkpad_e470					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3578
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3579
yangtian_afq150					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3580
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-YANG-271119/3581

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkpad_e570					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3582
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3583
yangtian_mc_h110					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3584
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3585
yangtian_mc_h110_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3586

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3587
yangtian_mc_h81					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3588
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3589
thinkpad_e480					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3590
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3591
thinkpad_e580					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3592

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3593
thinkpad_s5					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3594
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3595
yangtian_ytm6900e-00					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3596
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-YANG-271119/3597

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_l380					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3598
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3599
yta8900f					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YTA8-271119/3600
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YTA8-271119/3601
thinkpad_l380_yoga					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3602

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3603
thinkpad_l460					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3604
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3605
thinkpad_l470					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3606
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3607
thinkpad_l480					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3608
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3609
ideacentre_730s-24ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3610
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3611
qt_a7400					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QT_A-271119/3612
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-QT_A-271119/3613

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_l580					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3614
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3615
thinkpad_l560					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3616
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3617
thinkcentre_e74z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3618

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3619
thinkpad_l570					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3620
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3621
thinkcentre_e95z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3622
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3623

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkcentre_e96z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3624
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3625
thinkcentre_m7300z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3626
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3627
thinkpad_p50					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3628
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-THIN-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3629
thinkcentre_m820z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3630
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3631
thinkcentre_m8300z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3632
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3633
thinkpad_p50s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-THIN-271119/3634

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3635
thinkcentre_m8350z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3636
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3637
thinkpad_p51s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3638
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-THIN-271119/3639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6172		
aio520-24arr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO5-271119/3640
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO5-271119/3641
qitian_a815					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3642
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3643
thinkcentre_m9350z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3644

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3645
thinkcentre_m93z_\(aio\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3646
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3647
v540-24iwl\(yt_s5430\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V540-271119/3648
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V540-271119/3649
yogo_a940-27icb					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-YOGO-271119/3650

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YOGO-271119/3651
130-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-130--271119/3652
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-130--271119/3653
130-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-130--271119/3654
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-130--271119/3655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
330-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3656
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3657
330-15ich					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3658
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3659
330-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-330--271119/3660

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3661
330-17ich					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3662
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3663
330-17ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330--271119/3664
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330--271119/3665
330c-14ikb					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330C-271119/3666
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330C-271119/3667
330c-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330C-271119/3668
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-330C-271119/3669
330c-15ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-330C-271119/3670
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-330C-271119/3671

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
340c-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-340C-271119/3672
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-340C-271119/3673
530s-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-530S-271119/3674
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-530S-271119/3675
530s-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-530S-271119/3676

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-530S-271119/3677
530s-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-530S-271119/3678
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-530S-271119/3679
530s-15ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-530S-271119/3680
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-530S-271119/3681

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
720s-14ikbr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-720S-271119/3682
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-720S-271119/3683
730s-13iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-730S-271119/3684
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-730S-271119/3685
c340-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-C340-271119/3686
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-C340-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3687
c340-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-C340-271119/3688
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-C340-271119/3689
e42-80					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-E42--271119/3690
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-E42--271119/3691
e52-80					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-E52--271119/3692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-E52--271119/3693
flex_6-14ikb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-FLEX-271119/3694
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-FLEX-271119/3695
flex-14iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-FLEX-271119/3696
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-FLEX-271119/3697

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
flex-15iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-FLEX-271119/3698
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-FLEX-271119/3699
thinkpad_p52s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3700
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3701
thinkpad_p70					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3702

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3703
thinkpad_e560p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3704
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3705
thinkpad_t25					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3706
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3707
thinkpad_t460					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3708

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3709
thinkpad_t460p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3710
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3711
thinkpad_t460s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3712
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_t470					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3714
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3715
thinkpad_t470p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3716
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3717
thinkpad_t470s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3718

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3719
thinkpad_t480					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3720
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3721
thinkpad_t480s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3722
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3723
thinkpad_t560					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3724
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3725
thinkpad_t570					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3726
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3727
thinkpad_t580					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3728
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3729

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_x1_carbon					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3730
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3731
thinkpad_x1_yoga					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3732
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3733
thinkpad_x1_tablet					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3735
thinkpad_x260					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3736
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3737
thinkpad_x270					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3738
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3739

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_x280					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3740
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3741
thinkpad_x380_yoga					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3742
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3743
thinkcentre_m83z_\(aio\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3744
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-THIN-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3745
thinkcentre_m920z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3746
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3747
thinkcentre_m9500z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3748
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3749
thinkcentre_m9550z					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-THIN-271119/3750

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3751
thinkcentre_x1_aio					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3752
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3753
v310z\(yt_s3150\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V310-271119/3754
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-V310-271119/3755

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
v510z_\(yt_s5250\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V510-271119/3756
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V510-271119/3757
v530-22icb\(yt_s4350\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V530-271119/3758
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V530-271119/3759
v530-24icb\(yt_s5350\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V530-271119/3760

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V530-271119/3761
thinkstation_e32					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3762
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3763
thinkstation_p300					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3764
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3765
thinkstation_p310					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3766

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3767
thinkstation_p318					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3768
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3769
thinkstation_p320					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3770
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkstation_p320_tiny					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3772
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3773
thinkstation_p330					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3774
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3775
thinkstation_p330_tiny					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3776

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3777
510-15ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-510--271119/3778
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-510--271119/3779
510s-08ikl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-510S-271119/3780
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-510S-271119/3781
ideacentre_300-20ish					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3782
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3783
ideacentre_300s-11ish					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3784
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3785
ideacentre_510-15icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3786
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-IDEA-271119/3787

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
ideacentre_510a-15icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3788
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3789
ideacentre_510s-08ish					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3790
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3791
ideacentre_700					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-IDEA-271119/3792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3793
thinkpad_t440p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3794
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3795
thinkpad_t450					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3796
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3797

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_t450s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3798
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3799
thinkpad_t490					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3800
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3801
thinkpad_t490s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3802
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-THIN-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3803
thinkpad_t540p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3804
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3805
thinkpad_t550					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3806
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3807
thinkpad_t590					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-THIN-271119/3808

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3809
thinkpad_tablet_10					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3810
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3811
thinkpad_tablet_8					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3812
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-THIN-271119/3813

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkpad_w540					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3814
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3815
thinkpad_w541					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3816
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3817
thinkpad_w550s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3818

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3819
thinkpad_x1_extreme					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3820
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3821
thinkpad_x131e					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3822
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3823
thinkpad_x140e					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3824

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3825
thinkpad_x240					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3826
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3827
thinkpad_x240s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3828
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3829

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_x250					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3830
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3831
thinkpad_x390					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3832
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3833
thinkpad_x390_yoga					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3834

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3835
thinkpad_yoga_11e					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3836
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3837
thinkpad_yoga_260-s1					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3838
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3839
thinksystem_hr630x_\(skl\)					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3840
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3841
thinksystem_hr650x_\(skl\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3842
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3843
thinksystem_odc5200-cn650s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3844
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3845

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_yoga_370					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3846
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3847
thinkpad_s1_3rd					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3848
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3849
ideacentre_310s-08asr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-IDEA-271119/3850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3851
ideacentre_310s-08igm					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3852
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3853
ideacentre_720-18apr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-IDEA-271119/3854
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-IDEA-271119/3855

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
legion_t530-28apr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3856
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3857
legion_t530-28apr_reflash					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3858
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-LEGI-271119/3859
legion_t530-28icb_reflash					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-LEGI-271119/3860
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-LEGI-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3861
63					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-63-271119/3862
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-63-271119/3863
v330-15igm					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-V330-271119/3864
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V330-271119/3865
v530s-07icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-V530-271119/3866

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-V530-271119/3867
qitian_b5900					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-QITI-271119/3868
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-QITI-271119/3869
thinkcentre_e73					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3870
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-THIN-271119/3871

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkcentre_e93					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3872
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3873
thinkcentre_m600					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3874
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3875
thinkcentre_m625q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3876

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3877
thinkcentre_m715q					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3878
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3879
thinkcentre_m715q_rr					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3880
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3881
thinkcentre_m715t					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3882

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3883
thinkpad_e490					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3884
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3885
thinkpad_e590					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3886
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkpad_r490					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3888
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3889
thinkpad_r590					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3890
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3891
thinkpad_helix					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3892

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3893
thinkpad_s3_3rd_gen					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3894
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3895
thinkpad_s2_yoga_3rd_gen					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3896
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3897
thinkpad_l390_yoga					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3898
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3899
thinkpad_s2_yoga_4th_gen					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3900
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3901
thinkpad_l450					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3902
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-THIN-271119/3903

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
thinkpad_l490					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3904
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3905
thinkpad_l590					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3906
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3907
thinkpad_p1					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-THIN-271119/3908

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3909
thinkpad_p43s_\(20rx\)					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3910
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3911
thinkpad_p51					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3912
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3913

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkpad_p52					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3914
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3915
thinkpad_p53					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3916
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3917
thinkpad_p53s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3918
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-THIN-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3919
thinkpad_p71					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3920
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3921
thinkpad_p72					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3922
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3923
thinkpad_p73					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-THIN-271119/3924

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3925
thinkpad_s1_yoga					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3926
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3927
thinkpad_s5_2nd_generation					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3928
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-THIN-271119/3929

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
thinkpad_s5_yoga_15					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3930
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3931
thinkpad_s531					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3932
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3933
thinkpad_s540					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3934

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3935
thinkpad_t440					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3936
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3937
thinkpad_t440s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3938
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3939
thinkcentre_m715s					
Improper Input	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads	N/A	H-LEN-THIN-271119/3940

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3941
thinkcentre_m725s					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3942
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3943
thinkcentre_m73					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3944
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary	N/A	H-LEN-THIN-271119/3945

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution **CVE ID : CVE-2019-6172**		
thinkcentre_m79					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3946
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3947
thinkcentre_m83					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3948
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3949
thinkcentre_m90n-1					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances.	N/A	H-LEN-THIN-271119/3950

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6170		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3951
thinkcentre_m93p					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-THIN-271119/3952
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-THIN-271119/3953
yangtian_me_h110					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3954
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3955
yangtian_we_h110					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3956
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3957
yangtian_mf_h110_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3958
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3959
yangtian_wf_h110_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3960
Improper Input	12-11-2019	7.5	A potential vulnerability in the SMI callback function in	N/A	H-LEN-YANG-271119/3961

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		
yangtian_mf_h81_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3962
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3963
yangtian_wf_h81_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3964
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3965
yangtian_ms_h81					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under	N/A	H-LEN-YANG-271119/3966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3967
yangtian_ws_h81					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3968
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3969
yangtian_tc_h110_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3970
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3971

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
yangtian_wc_h110_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3972
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3973
yangtian_tc_h81_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3974
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-YANG-271119/3975
yangtian_wcc_h81_pci					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-YANG-271119/3976
Improper	12-11-2019	7.5	A potential vulnerability in	N/A	H-LEN-YANG-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**		271119/3977
a340-22_iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-A340-271119/3978
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-A340-271119/3979
a340-24_iwl					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-A340-271119/3980
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-A340-271119/3981
a340-22icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to	N/A	H-LEN-A340-271119/3982

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**		
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-A340-271119/3983
a340-24icb					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-A340-271119/3984
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-A340-271119/3985
a340-22ast					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-A340-271119/3986
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution	N/A	H-LEN-A340-271119/3987

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-6172		
aio_330-20ast					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO_-271119/3988
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO_-271119/3989
aio_330-20igm					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO_-271119/3990
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO_-271119/3991
aio_520-24ast					
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in some Lenovo ThinkPads may allow an attacker to execute arbitrary code under SMM under certain circumstances. **CVE ID : CVE-2019-6170**	N/A	H-LEN-AIO_-271119/3992

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	12-11-2019	7.5	A potential vulnerability in the SMI callback function in some Lenovo ThinkPad models may allow arbitrary code execution **CVE ID : CVE-2019-6172**	N/A	H-LEN-AIO_-271119/3993
Medtronic					
valleylab_ft10_energy_platform					
Improper Authentication	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism used for authentication between the FT10/LS10 Energy Platform and instruments can be bypassed, allowing for inauthentic instruments to connect to the generator. **CVE ID : CVE-2019-13531**	N/A	H-MED-VALL-271119/3994
Information Exposure	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism does not apply read protection, allowing for full read access of the RFID security mechanism data.	N/A	H-MED-VALL-271119/3995

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-13535		
Improper Input Validation	08-11-2019	7.2	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use the descrypt algorithm for OS password hashing. While interactive, network-based logons are disabled, and attackers can use the other vulnerabilities within this report to obtain local shell access and access these hashes. **CVE ID : CVE-2019-13539**	N/A	H-MED-VALL-271119/3996
Use of Hard-coded Credentials	08-11-2019	5	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use multiple sets of hard-coded credentials. If discovered, they can be used to read files on the device. **CVE ID : CVE-2019-13543**	N/A	H-MED-VALL-271119/3997
valleylab_ls10_energy_platform					
Improper Authentication	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3	N/A	H-MED-VALL-271119/3998

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism used for authentication between the FT10/LS10 Energy Platform and instruments can be bypassed, allowing for inauthentic instruments to connect to the generator. **CVE ID : CVE-2019-13531**		
Information Exposure	08-11-2019	2.1	In Medtronic Valleylab FT10 Energy Platform (VLFT10GEN) version 2.1.0 and lower and version 2.0.3 and lower, and Valleylab LS10 Energy Platform (VLLS10GEN?not available in the United States) version 1.20.2 and lower, the RFID security mechanism does not apply read protection, allowing for full read access of the RFID security mechanism data. **CVE ID : CVE-2019-13535**	N/A	H-MED-VALL-271119/3999
valleylab_fx8_energy_platform					
Improper Input Validation	08-11-2019	7.2	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use the descrypt algorithm for OS password	N/A	H-MED-VALL-271119/4000

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hashing. While interactive, network-based logons are disabled, and attackers can use the other vulnerabilities within this report to obtain local shell access and access these hashes. **CVE ID : CVE-2019-13539**		
Use of Hard-coded Credentials	08-11-2019	5	Medtronic Valleylab Exchange Client version 3.4 and below, Valleylab FT10 Energy Platform (VLFT10GEN) software version 4.0.0 and below, and Valleylab FX8 Energy Platform (VLFX8GEN) software version 1.1.0 and below use multiple sets of hard-coded credentials. If discovered, they can be used to read files on the device. **CVE ID : CVE-2019-13543**	N/A	H-MED-VALL-271119/4001
patriotmemory					
viper_rgb					
Improper Privilege Management	09-11-2019	3.6	The MsIo64.sys and MsIo32.sys drivers in Patriot Viper RGB before 1.1 allow local users (including low integrity processes) to read and write to arbitrary memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, by mapping \Device\PhysicalMemory into the calling process via ZwOpenSection and ZwMapViewOfSection. **CVE ID : CVE-2019-18845**	N/A	H-PAT-VIPE-271119/4002

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Qualcomm					
mdm9206					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4003
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4004

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4005

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10504		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4006
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4007

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4008

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4009
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4010

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4011
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	H-QUA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	MDM9-271119/4012
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4013

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4014
Improper Restriction	06-11-2019	10	Dereference on uninitialized buffer can happen when	https://source.android.	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	com/security/bulletin/	271119/4015
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4016

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4017
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MDM9-271119/4018

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4019

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 430, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 636, 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4020
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4021

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4022

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4023
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4024

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4025

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
mdm9607					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4026

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4027
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4028

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4029
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	MDM9-271119/4030
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4031

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4032
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	H-QUA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	MDM9-271119/4033
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4034

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4035
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4036

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4037
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4038

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4039

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4040
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4042

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MDM9-271119/4043
Improper Restriction	06-11-2019	10	Improper validation of read and write index of tx and rx	https://source.android.	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	com/security/bulletin/	271119/4044
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4045

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4046
Improper Restriction of Operations	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4047

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4048

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4049
Improper Restriction of	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated	https://source.android.com/securit	H-QUA-MDM9-271119/4050

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	y/bulletin/	
msm8909w					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4051

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4052

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4053
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4054

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4055
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4056

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4057

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4058
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4059

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4060

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4061
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4062

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4063

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10529		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4064
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4065

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4066
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4067

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4068
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4069

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MSM8-271119/4070

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4071

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4072
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4073

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4074

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4075
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4076

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4077

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4078
msm8996au					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4079

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4080

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4081
Buffer Copy without Checking	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data	https://source.android.com/securit	H-QUA-MSM8-271119/4082

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			structure leads to buffer overflow 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-2019-10496**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4083

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4084

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4086

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4087

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4088
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4089

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4090
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4091

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4092

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4093
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4094

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4095

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-MSM8-271119/4096

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4097
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4098

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4099

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4100
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4101

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4102

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/4103
qca6574au					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4104

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4105

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4106
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4107

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4108

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4109
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4110

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/4111

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qcs405					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4112
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4113

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4114

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10502		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4115
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4116

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4117

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4118
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4119

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4120
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	H-QUA-QCS4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/4121
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4122

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4123
Improper Restriction	06-11-2019	10	Dereference on uninitialized buffer can happen when	https://source.android.	H-QUA-QCS4-271119/4124

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	com/security/bulletin/	
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845,	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4125

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4126
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4127

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4128

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4129
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-QCS4-271119/4130

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
qcs605					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4131

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4132
Improper	06-11-2019	4.6	Arbitrary buffer write issue	https://sou	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	rce.android.com/security/bulletin/	271119/4133
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4134

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4135
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4136

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4137

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4138
Concurrent Execution using Shared Resource with Improper Synchroniza	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4139

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion ('Race Condition')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4140

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4141
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4142

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4143
Improper Restriction of Operations	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4144

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4145

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4146
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key	https://www.qualcomm.com/company/product-	H-QUA-QCS6-271119/4147

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4148

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4149

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2285**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4150
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4151

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4152

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4153
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-QCS6-271119/4154

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
qualcomm_215					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4155

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4156

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10491		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4157
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4158

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4159
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4160

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4161

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4162
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4163

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4164

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4165
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4166

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10533		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4167
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4168

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4169
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory	https://source.android.com/securit	H-QUA-QUAL-271119/4170

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	y/bulletin/	
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-QUAL-271119/4171

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4172

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 625, SD 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4173
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by	https://source.android.	H-QUA-QUAL-271119/4174

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user is initialized can result in bus error 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, 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-2019-2323**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4175

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4176

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-QUAL-271119/4177
sd_210					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4178

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4179

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4180
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4181

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4182
Uncontrolle	06-11-2019	5	Firmware not able to send	https://sou	H-QUA-SD_2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d Resource Consumption			EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	rce.android.com/security/bulletin/	271119/4183
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4184

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 650/52, 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-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4185
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring	https://source.android.com/securit	H-QUA-SD_2-271119/4186

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	y/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4187

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4188
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4189

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4190

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4191
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4192

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4193
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4194

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4195
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	H-QUA-SD_2-271119/4196

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_2-271119/4197

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4198

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4199
N/A	06-11-2019	10	Lack of check to ensure	https://sou	H-QUA-SD_2-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	rce.android.com/security/bulletin/	271119/4200
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4201

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4202
Integer Overflow or Wraparoun	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if	https://source.android.com/securit	H-QUA-SD_2-271119/4203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	y/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4204

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
sd_212					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4205

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4206
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4207

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4208

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4209
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4210

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4211
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4212

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4213

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4214
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4215

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4216

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4217
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4218

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4219
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4220

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4221

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4222
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4223

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_2-271119/4224

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4225
Out-of-bounds	06-11-2019	10	Out of bound write issue is observed while giving	https://source.android.	H-QUA-SD_2-271119/4226

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			information about properties that have been set so far for playing video 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-2019-2285**	com/security/bulletin/	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4227

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4228
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4229

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4230

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4231

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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_205					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4232
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4233

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4234

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4235
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4236

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4237
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4238

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4239

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4240
Buffer Copy without Checking Size of Input ('Classic Buffer	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4241

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 /	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4242

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4243
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4244

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4245
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4246

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4247

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10534		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4248
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4249

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4250

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_2-271119/4251
Improper	06-11-2019	10	Improper validation of read	https://sou	H-QUA-SD_2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	rce.android.com/security/bulletin/	271119/4252
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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,	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4253

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4254
Improper Restriction	06-11-2019	10	When ADSP is compromised, the audio port index that`s	https://source.android.	H-QUA-SD_2-271119/4255

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4256

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_2-271119/4257
Improper	06-11-2019	10	Memory corruption while	https://sou	H-QUA-SD_2-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	rce.android.com/security/bulletin/	271119/4258
sd_425					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4259

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4260

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4261
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4262

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4263
Uncontrolled Resource	06-11-2019	5	Firmware not able to send EXT scan response to host	https://source.android.	H-QUA-SD_4-271119/4264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	com/security/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4265

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4266
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4267

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4268

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4269
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4270

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4271

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4272
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4273

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10533		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4274
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4275

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4276
Improper Restriction of	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location	https://source.android.com/securit	H-QUA-SD_4-271119/4277

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4278

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/4279

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4280
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4281

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4282

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4283
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4284

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4285

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4286
sd_427					
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	271119/4287
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4288

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4289

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4290
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4291

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4292
Use After	06-11-2019	4.9	DCI client which might be	https://sou	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	rce.android.com/security/bulletin/	271119/4293
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4294

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4295
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4296

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4297

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4298
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4299

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4300
Out-of-	06-11-2019	10	Kernel can do a memory	https://sou	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	rce.android.com/security/bulletin/	271119/4301
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W, MSM8996AU, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4302

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/4303

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4304
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4305

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4306

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4307
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4308

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4309

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4310
sd_430					
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	271119/4311
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4312

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4313

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4314
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4315

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 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4316
Use After	06-11-2019	4.9	DCI client which might be	https://sou	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	rce.android.com/security/bulletin/	271119/4317
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4318

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4319
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4320

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4321

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4322
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4323

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4324

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-SD_4-271119/4325

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4326
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4327

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4328

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4329
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4330

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4331

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4332
sd_435					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4333

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4334

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4335
Buffer Copy without Checking Size of Input	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4336

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			overflow 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-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4337

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4338
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4339

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4340

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4341
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4342

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4343
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is	https://source.android.com/securit	H-QUA-SD_4-271119/4344

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4345

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4346
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4347

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4348

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-SD_4-271119/4349

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4350
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4351

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4352

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4353
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4354

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4355

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4356
sd_439					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4357

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4358

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4359
Buffer Copy without Checking Size of Input	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4360

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			overflow 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4361

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4362
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4363

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4364

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10512		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4365
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4366

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4367
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/4368
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4369

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4370
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4371

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4372
Improper Restriction of Operations	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4373

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4374

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 /	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/4375

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4376
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4377

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4378

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4379
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4380

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4381

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_429					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4382

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4383
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4384

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4385

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4386
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4387

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10504		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4388
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4389

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4390

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4391
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4392

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4393

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4394
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4395

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4396
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4398
Improper	06-11-2019	10	Improper validation of array	https://sou	H-QUA-SD_4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	rce.android.com/security/bulletin/	271119/4399
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/4400

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4401

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4402

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4403
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4404

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4405

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4406
sd_450					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4407

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4408

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4409
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4410

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4411

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10502		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4412
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4413

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4414

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4416

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4417
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its	https://source.android.com/securit	H-QUA-SD_4-271119/4418

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	y/bulletin/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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 /	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4419

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4420
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4421

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4422
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4423

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4424

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10542		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4425
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4426

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4427

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/4428
Improper Restriction	06-11-2019	10	Improper validation of read and write index of tx and rx	https://source.android.	H-QUA-SD_4-271119/4429

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	com/security/bulletin/	
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4430

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4431
Improper Restriction of	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might	https://source.android.com/securit	H-QUA-SD_4-271119/4432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4433

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4434
Improper Restriction	06-11-2019	10	Memory corruption while accessing the memory as	https://source.android.	H-QUA-SD_4-271119/4435

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	com/security/bulletin/	
sd_600					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4436

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4437

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10522		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4438
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4439

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, 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 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4440
Out-of-bounds	06-11-2019	7.5	Buffer over-read may occur when downloading a	https://source.android.	H-QUA-SD_6-271119/4441

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4442

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4443
Improper Restriction of Operations	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4444

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_615					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, QCA6574AU,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4445

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4446

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4447
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4448

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4449

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4450
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4451

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4452

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4453
Integer	06-11-2019	10	Possible Integer overflow	https://sou	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	rce.android.com/security/bulletin/	271119/4454
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4455

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_616					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4456

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4457
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4458

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4459

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10522**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4460
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4461

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4462

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4463

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4464
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4465

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_415					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4466

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4467
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4468

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4469

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4470

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4471
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4472

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4473

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4474
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4475

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_4-271119/4476

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2332**		
sd_625					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4477
Buffer Copy without Checking Size of Input	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto,	https://source.android.com/securit	H-QUA-SD_6-271119/4478

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	y/bulletin/	
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4479

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4480
Buffer Copy	06-11-2019	4.6	Possible stack overflow	https://sou	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	rce.android.com/security/bulletin/	271119/4481
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4482
Out-of-bounds	06-11-2019	7.5	Out of bound access while processing a non-standard	https://source.android.	H-QUA-SD_6-271119/4483

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4484

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4485

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10515		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4486
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4487

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4488
Concurrent Execution using Shared	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4489

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4490
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table	https://source.android.com/securit	H-QUA-SD_6-271119/4491

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	y/bulletin/	
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4492

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4493
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4494

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4495

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4496
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4497

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU, QCS404, QCS605, Qualcomm	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_6-271119/4498

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4499
Out-of-	06-11-2019	10	Out of bound write issue is	https://sou	H-QUA-SD_6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			observed while giving information about properties that have been set so far for playing video 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-2019-2285**	rce.android.com/security/bulletin/	271119/4500
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4501

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4502
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without	https://source.android.com/securit	H-QUA-SD_6-271119/4503

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	y/bulletin/	
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4504

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4505

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2332		
sd_632					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4506
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4507

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4508

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4510

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4511
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4512

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4513

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4514
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4516

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4517
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4518

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4519
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4520

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4521

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4522
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key	https://www.qualcomm.com/company/produ	H-QUA-SD_6-271119/4523

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	ct-security/bulletins	
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4524

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4525

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4526
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4528

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4529
sd_636					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in	https://source.android.com/securit	H-QUA-SD_6-271119/4530

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**	y/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4531

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4532

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4533
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4534

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4535
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4536

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4537

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4538
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4539

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4540

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4541
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4542

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4543

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4544
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4545

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4546
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4547

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) 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	H-QUA-SD_6-271119/4548

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4549

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4550
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4551

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4552

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4553
Improper Restriction	06-11-2019	10	Memory corruption while accessing the memory as	https://source.android.	H-QUA-SD_6-271119/4554

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	com/security/bulletin/	
sd_665					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4555

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4556

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4557
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4558

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4559
Uncontrolled Resource Consumptio	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource	https://source.android.com/securit	H-QUA-SD_6-271119/4560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	y/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4561

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4562
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4563

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4564

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4565
Concurrent Execution using Shared Resource with Improper Synchroniza	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4566

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion ('Race Condition')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4567

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4568
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4569

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4570

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2246		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4571
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9650, MDM9655, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4572

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2258**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4573

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4574
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4575

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4576

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4577
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_675					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4579

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4580
Improper	06-11-2019	4.6	Arbitrary buffer write issue	https://sou	H-QUA-SD_6-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	rce.android.com/security/bulletin/	271119/4581
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4582

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4583
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4584

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4585

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4586
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4587

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4588

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4589
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4590

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4591

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10533		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4592
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4593

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4594
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during	https://source.android.com/securit	H-QUA-SD_6-271119/4595

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4596

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4597
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about	https://source.android.com/securit	H-QUA-SD_6-271119/4598

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properties that have been set so far for playing video 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-2019-2285**	y/bulletin/	
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4599

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4600
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4601

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4602

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4603
sd_712					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4604
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4605

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4606

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4608

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4609
Improper Validation of	06-11-2019	4.6	Payload size is not checked before using it as array index	https://source.android.	H-QUA-SD_7-271119/4610

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	com/security/bulletin/	
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4611

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4612
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is	https://source.android.	H-QUA-SD_7-271119/4613

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	com/security/bulletin/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4614

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4615
NULL Pointer	06-11-2019	10	Null-pointer dereference can occur while accessing the	https://source.android.	H-QUA-SD_7-271119/4616

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4617

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4618
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4620

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2249		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4621
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_7-271119/4622

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4623

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4624

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4625
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4626

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4627

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4628
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4629

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_710					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4630

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4631
Improper Input	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence	https://source.android.	H-QUA-SD_7-271119/4632

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			header during HEVC or AVC encoding. 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-2019-10495**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4633

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4634
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4636

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4637
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4638

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4639

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4640
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4641

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4642

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4643
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4644

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4645
Out-of-bounds	06-11-2019	10	Kernel can do a memory read from arbitrary address	https://source.android.	H-QUA-SD_7-271119/4646

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4647

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 /	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_7-271119/4648

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4649
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4650

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4651

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4652
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4653

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4654

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4655
sd_670					
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the	https://source.android.com/securit	H-QUA-SD_6-271119/4656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			nonstandard clip 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, 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 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-2019-10488**	y/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4657

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4658

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4659
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4661
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4662

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4663

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4664
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4665

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4666

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4667
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4668

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4669

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4670
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4671

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4672
Improper	06-11-2019	10	Improper validation of array	https://sou	H-QUA-SD_6-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	rce.android.com/security/bulletin/	271119/4673
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_6-271119/4674

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4675

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4676

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4677
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4678

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4679
Integer Overflow or	06-11-2019	10	Possible Integer overflow because of subtracting two	https://source.android.	H-QUA-SD_6-271119/4680

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/4681

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_730					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4682

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4683
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4684

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4685

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4686
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4687

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4688

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4689
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4690

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4691

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10524		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4692
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4693

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4694
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is	https://source.android.com/securit	H-QUA-SD_7-271119/4695

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	y/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4696

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4697
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4698

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4699

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4700
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4701

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4702

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4703
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4704

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4705

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_7-271119/4706
sd_820					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4707

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4708

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4709
Buffer Copy	06-11-2019	4.6	Lack of checking a variable	https://sou	H-QUA-SD_8-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	rce.android.com/security/bulletin/	271119/4710
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4711

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4712

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4713
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4714

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4715
Concurrent Execution using Shared Resource with	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4716

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Synchronization ('Race Condition')			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4717

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4718
Improper Restriction of Operations within the Bounds of a Memory	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4719

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4720

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4721
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4722

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_8-271119/4723

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4724

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2283		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4725
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4726

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4727

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4728
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4729

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4730

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
sd_820a					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4731
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4732

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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 /	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4733

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4734
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4735

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4736

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4737
Buffer Copy without	06-11-2019	7.5	While playing the clip which is nonstandard buffer	https://source.android.	H-QUA-SD_8-271119/4738

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	com/security/bulletin/	
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4739

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4740
Concurrent Execution using Shared Resource with Improper Synchroniza	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4741

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tion ('Race Condition')			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4742

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4743
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4744

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4745

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10542		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4746
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_8-271119/4747

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4748

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4749

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4750
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4751

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4752

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4753
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4754

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sd_835					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4755

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4756
Improper Input	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence	https://source.android.	H-QUA-SD_8-271119/4757

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			header during HEVC or AVC encoding. 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-2019-10495**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4758

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4759
Improper	06-11-2019	4.6	Payload size is not checked	https://sou	H-QUA-SD_8-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	rce.android.com/security/bulletin/	271119/4760
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4761

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4762
Use After	06-11-2019	4.6	Lack of check for a negative	https://sou	H-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	rce.android.com/security/bulletin/	271119/4763
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4764

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4765
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4766

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4767

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4768
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4769

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4770
Improper	06-11-2019	10	Improper validation of array	https://sou	H-QUA-SD_8-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	rce.android.com/security/bulletin/	271119/4771
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_8-271119/4772

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4773

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4774

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4775
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4776

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4777

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4778
sd_845					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4779

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4780

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4781
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4782

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4783

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10502		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4784
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4785

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4786

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4787
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4788

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4789
Concurrent Execution using	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry	https://source.android.com/securit	H-QUA-SD_8-271119/4790

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4791

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4792
Improper Restriction of Operations	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4793

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4794

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4795
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4796

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4797

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-SD_8-271119/4798

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4799
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4800

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4801

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2323		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4802
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4803

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4804

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4805
sd_850					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4806

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4807

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4808
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4809

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4810

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10502		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4811
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4812

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4813

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4814
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4815

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4816
Concurrent Execution using	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry	https://source.android.com/securit	H-QUA-SD_8-271119/4817

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('Race Condition')			pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4818

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4819
Improper Restriction of Operations	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4820

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4821

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4822
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4823

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4824

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-SD_8-271119/4825

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4826
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4827

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4828

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2323		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4829
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4830

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4831

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4832
sd_855					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4833

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4834

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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-2019-10495**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4835
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4836

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			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-2019-10496**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4837

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10502		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4838
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4839

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4840

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4841
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4842

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4843
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	H-QUA-SD_8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	271119/4844
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4845

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4846
Improper Restriction	06-11-2019	10	Dereference on uninitialized buffer can happen when	https://source.android.	H-QUA-SD_8-271119/4847

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4848

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4849
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_8-271119/4851

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4852

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4853
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4854

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4855

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4856
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4857

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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 /	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/4858

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2332**		
sda660					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4859
Buffer Copy without Checking Size of Input ('Classic	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4860

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4861

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4862
Uncontrolled Resource	06-11-2019	5	Firmware not able to send EXT scan response to host	https://source.android.	H-QUA-SDA6-271119/4863

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	com/security/bulletin/	
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 665, SD 675,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4864

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4865
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4866

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4867

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4868
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4869

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4870

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4871
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4872

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4873
Improper	06-11-2019	7.2	Thread start can cause	https://sou	H-QUA-SDA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	rce.android.com/security/bulletin/	271119/4874
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4875

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4876
Improper Input	06-11-2019	2.1	While deserializing any key blob during key operations,	https://www.qualcom	H-QUA-SDA6-271119/4877

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	m.com/company/product-security/bulletins	
Improper Restriction of Operations within the Bounds of a	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4878

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4879

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4880
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4882

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SDA6-271119/4883
sdm439					
NULL Pointer	06-11-2019	5	Null pointer dereference can occur while parsing invalid	https://source.android.	H-QUA-SDM4-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			chunks while playing the nonstandard clip 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, 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 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-2019-10488**	com/security/bulletin/	271119/4884
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4885

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4886

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4888

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4889
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4890

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4891

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4893

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4894

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	10	Incorrect reading of system image resulting in buffer overflow when size of system image is increased in Snapdragon Auto, Snapdragon Mobile, Snapdragon Wearables in MDM9607, MSM8909W, Qualcomm 215, SD 210/SD	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4896

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SDM439 **CVE ID : CVE-2019-10531**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4897
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4898

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4899

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10541		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4900
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M,	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4901

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SDM4-271119/4902

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS404, QCS605, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4903

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4904
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4905

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, 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-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4906

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4907
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDM4-271119/4908

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
sdm630					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4909

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4910
Improper Input	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence	https://source.android.	H-QUA-SDM6-271119/4911

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			header during HEVC or AVC encoding. 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-2019-10495**	com/security/bulletin/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4912

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4913
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4914

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4915

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4916
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4917

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4918

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4919
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4920

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4921

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10533		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10534**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4922
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4923

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4924
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during	https://source.android.com/securit	H-QUA-SDM6-271119/4925

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	y/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4926

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SDM6-271119/4927

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4928
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4929

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon 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-2019-2285**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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 /	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4930

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 670, SD 730, SD 820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-2323**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4931
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4932

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4933

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
sdm660					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4934

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4935
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4936

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4937

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10496**		
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4938
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4939

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4940

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10512		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4941
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4942

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 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-2019-10522**		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4943
Use After	06-11-2019	7.5	Use after free issue in kernel	https://sou	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	rce.android.com/security/bulletin/	271119/4944
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4945

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-10529**		
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, 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-2019-10533**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4946
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4947

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4948

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10541**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4949
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4950

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4951

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SDM6-271119/4952

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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 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-2019-2283**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4953
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4954

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2285**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4955

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4956
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4957

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4958

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/4959
sdx20					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4960

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, 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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4961

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-10491**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4962
Improper Validation of	06-11-2019	4.6	Payload size is not checked before using it as array index	https://source.android.	H-QUA-SDX2-271119/4963

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	com/security/bulletin/	
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4964

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCS405, 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-2019-10515**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	7.5	While playing the clip which is nonstandard buffer overflow can occur while parsing in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 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-2019-10522**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4965
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is	https://source.android.	H-QUA-SDX2-271119/4966

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	com/security/bulletin/	
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4967

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4968
Improper Validation of Array Index	06-11-2019	10	Out of bound access due to improper validation of array index cause the index table entry to get corrupt in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4969

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9206, MDM9607, 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 600, 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-2019-10533**		
NULL Pointer Dereference	06-11-2019	10	Null-pointer dereference can occur while accessing the super index entry when it is not been allocated in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, 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 600, SD 625, SD 632, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4970

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			820, SD 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20 **CVE ID : CVE-2019-10534**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Dereference on uninitialized buffer can happen when parsing FLV clip with corrupted codec specific data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 600, 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-2019-10541**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4971
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4972

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4973
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	H-QUA-SDX2-271119/4974

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4975

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4976

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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-2019-2323**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4977
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4978

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4979

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2325		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4980
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/4981

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**		
mdm9150					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 600, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4982

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 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-2019-10488**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4983
Out-of-bounds	06-11-2019	7.5	Out of bound access while processing a non-standard	https://source.android.	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	com/security/bulletin/	271119/4984
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4985

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4986

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10515		
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4987
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4988

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4989

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10542		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4990
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MDM9-271119/4991

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4992

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, 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 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-2019-2283**		
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error 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, 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://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4993

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2323		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4994
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4995

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, 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, SDX24 **CVE ID : CVE-2019-2325**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4996

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4997
mdm9640					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4998

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/4999

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5000

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5001
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5002

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5003
Concurrent Execution using Shared Resource with Improper	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5004

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5005

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5006
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5007

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5008

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5009
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5010

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5011

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5012
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5013

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5014

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2332**		
mdm9650					
NULL Pointer Dereference	06-11-2019	5	Null pointer dereference can occur while parsing invalid chunks while playing the nonstandard clip 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, 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 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-2019-10488**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5015
Buffer Copy without Checking	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted	https://source.android.com/securit	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	y/bulletin/	271119/5016
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5017

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5018

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5019
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5020

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5021
Concurrent	06-11-2019	9.3	Possible use after free issue	https://sou	H-QUA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Execution using Shared Resource with Improper Synchronization ('Race Condition')			due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**	rce.android.com/security/bulletin/	MDM9-271119/5022
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5023

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5024
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5025

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MDM9-271119/5026

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, 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,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5027

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 636, 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5028
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5029

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5030

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5031
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5032

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5033

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-2332**		
sdx24					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5034

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Possible stack overflow when an index equal to io buffer size is accessed in camera module in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MSM8909W, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 625, SD 632, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 845 / SD 850, SD 855, SDM439, SDX24 **CVE ID : CVE-2019-10502**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5035
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5036

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 650/52, 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-2019-10505**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5037
Use After Free	06-11-2019	4.9	DCI client which might be preemptively freed up might be accessed for transferring	https://source.android.com/securit	H-QUA-SDX2-271119/5038

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets leading to kernel error in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, 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-2019-10515**	y/bulletin/	
Use After Free	06-11-2019	4.6	Lack of check for a negative value returned for get_clk is wrongly interpreted as valid pointer and lead to use after free in clk driver in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5039

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX24 **CVE ID : CVE-2019-10524**		
Use After Free	06-11-2019	7.5	Use after free issue in kernel while accessing freed mdlog session info and its attributes after closing the session in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 625, SD 636, SD 675, SD 730, SD 820, SD 820A, SD 835, SD 855, SDA660, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10528**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5040
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	06-11-2019	9.3	Possible use after free issue due to race condition while attempting to mark the entry pages as dirty using function set_page_dirty() in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5041

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, 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, SDX24 **CVE ID : CVE-2019-10529**		
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5042
Improper Restriction	06-11-2019	7.2	Thread start can cause invalid memory writes to	https://source.android.	H-QUA-SDX2-271119/5043

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	com/security/bulletin/	
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Improper validation of read and write index of tx and rx fifo`s before calculating pointer can lead to out-of-bound access 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, QCS605, Qualcomm 215, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 439 / SD	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5044

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			429, SD 450, SD 625, SD 632, SD 636, 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-2019-2283**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5045
N/A	06-11-2019	10	Lack of check to ensure crypto engine data passed by user is initialized can result in bus error in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5046

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 MDM9150, MDM9206, MDM9607, MDM9640, 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 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-2019-2323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5047

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Improper Validation of Array Index	06-11-2019	10	Out of boundary access due to token received from ADSP and is used without validation as an index into the array in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2325**	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5048
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5049

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-SDX2-271119/5050

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDX24 **CVE ID : CVE-2019-2332**		
ipq4019					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24	https://source.android.com/security/bulletin/	H-QUA-IPQ4-271119/5051

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10491		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-IPQ4-271119/5052
ipq8064					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-IPQ8-271119/5053

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCS405, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-IPQ8-271119/5054

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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, SDX20, SDX24, SXR1130 **CVE ID : CVE-2019-10512**		
ipq8074					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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	https://source.android.com/security/bulletin/	H-QUA-IPQ8-271119/5055

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10491**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-IPQ8-271119/5056
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-IPQ8-271119/5057

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
qca6174a					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/5058

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 650/52, 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-2019-10505**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/5059
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/5060

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qca9377					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, SD 439 / SD	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5061

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5062
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5063

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qca9379					
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5064

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**		
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5065
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and	https://source.android.com/security/bulletin/	H-QUA-QCA9-271119/5066

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sd_650					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5067

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5068
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5069

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_6-271119/5070

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
sd_652					
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660,	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5071

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Out-of-bounds Read	06-11-2019	7.5	Out of bound access while processing a non-standard IE measurement request with length crossing past the size of frame in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCS405, SD 210/SD 212/SD 205, SD 425, 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 820A, SD 835, SD 845 / SD 850, SD 855, SDA660, SDM439, SDM630, SDM660, SDX20, SDX24 **CVE ID : CVE-2019-10505**	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5072
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-SD_6-271119/5073

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_6-271119/5074

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
snapdragon_high_med_2016					
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. 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	https://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5075

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			850, SD 855, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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-2019-10496**	https://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5076
Uncontrolled Resource Consumption	06-11-2019	5	Firmware not able to send EXT scan response to host within 1 sec due to resource consumption issue in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5077

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Wearables in MDM9206, MDM9607, MSM8909W, 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 665, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016 **CVE ID : CVE-2019-10504**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5078
Out-of-bounds	06-11-2019	10	Kernel can do a memory read from arbitrary address	https://source.android.	H-QUA-SNAP-271119/5079

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5080

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 /	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SNAP-271119/5081

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 710 / SD 670, 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-2019-2275**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SNAP-271119/5082
sd616					
Buffer Copy without Checking	06-11-2019	4.6	ADSP can be compromised since it`s a general-purpose CPU processing untrusted	https://source.android.com/securit	H-QUA-SD61-271119/5083

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			data in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24 **CVE ID : CVE-2019-10491**	y/bulletin/	
apq8053					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-APQ8-271119/5084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-APQ8-271119/5085
mdm9207c					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some	https://source.android.com/securit	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	y/bulletin/	271119/5086
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5087

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
msm8905					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/5088
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/5089

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
qcn7605					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-QCN7-271119/5090
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity,	https://source.android.com/security/bulletin/	H-QUA-QCN7-271119/5091

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sdm845					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**	https://source.android.com/security/bulletin/	H-QUA-SDM8-271119/5092

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-SDM8-271119/5093
apq8017					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://source.android.com/security/bulletin/	H-QUA-APQ8-271119/5094

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
apq8096au					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670,	https://source.android.com/security/bulletin/	H-QUA-APQ8-271119/5095

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
msm8976					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/5096
sda845					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer	https://source.android.com/security/bulletin/	H-QUA-SDA8-271119/5097

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sdm636					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976,	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/5098

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
sdm670					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-SDM6-271119/5099
sdm710					
Integer Overflow or	06-11-2019	7.5	While processing vendor command which contains	https://source.android.	H-QUA-SDM7-271119/5100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	com/security/bulletin/	
qca6574					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD	https://source.android.com/security/bulletin/	H-QUA-QCA6-271119/5101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
qca8081					
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-QCA8-271119/5102
qcs404					
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur	https://www.qualcomm.com/com	H-QUA-QCS4-271119/5103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**	pany/product-security/bulletins	
sd_8cx					
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5105

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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, SD 8CX, SDA660, SDM439, SDM630, SDM660, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-10496**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5106
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5107

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**		
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5108

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			855, SD 8CX, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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	H-QUA-SD_8-271119/5109

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-2275**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SD_8-271119/5110
sxr1130					
Improper Input Validation	06-11-2019	4.6	Arbitrary buffer write issue while processing sequence header during HEVC or AVC encoding. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5111

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in 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-2019-10495**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	06-11-2019	4.6	Lack of checking a variable received from driver and populating in Firmware data structure leads to buffer overflow 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://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5112

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-10496**		
Improper Validation of Array Index	06-11-2019	4.6	Payload size is not checked before using it as array index in audio in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9607, MDM9640, 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, SDX24, SXR1130 **CVE ID : CVE-2019-10512**	https://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5113
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5114

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, 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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**	https://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5115
Out-of-bounds	06-11-2019	10	Kernel can do a memory read from arbitrary address	https://source.android.	H-QUA-SXR1-271119/5116

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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			passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	com/security/bulletin/	
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5117

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 /	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SXR1-271119/5118

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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 710 / SD 670, 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-2019-2275**		
Out-of-bounds Write	06-11-2019	10	Out of bound write issue is observed while giving information about properties that have been set so far for playing video 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-2019-2285**	https://source.android.com/security/bulletin/	H-QUA-SXR1-271119/5119
sm6150					
Integer Overflow or Wraparoun	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an	https://source.android.com/securit	H-QUA-SM61-271119/5120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d			integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	y/bulletin/	
sm8150					
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206,	https://source.android.com/security/bulletin/	H-QUA-SM81-271119/5121

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**		
mdm9615					
Out-of-bounds Read	06-11-2019	7.5	Buffer over-read may occur when downloading a corrupted firmware file that has chunk length in header which doesn`t match the contents in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 625, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 845 / SD 850, SDX20 **CVE ID : CVE-2019-10542**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5122
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	271119/5123
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	When ADSP is compromised, the audio port index that`s returned from ADSP might be out of the valid range and leads to out of boundary access in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5124

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in MDM9150, MDM9206, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, SD 210/SD 212/SD 205, SD 425, SD 427, SD 430, SD 435, SD 450, SD 600, SD 615/16/SD 415, SD 625, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 820, SD 820A, SD 845 / SD 850, SD 855, SDX20, SDX24 **CVE ID : CVE-2019-2324**		
Integer Overflow or Wraparound	06-11-2019	10	Possible Integer overflow because of subtracting two integers without checking if the result would overflow or not 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, MDM9640, 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,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5125

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24 **CVE ID : CVE-2019-2331**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	10	Memory corruption while accessing the memory as payload size is not validated before access 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, MDM9640, 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, SDX24 **CVE ID : CVE-2019-2332**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5126
mdm9625					
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5127

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**		
mdm9205					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-11-2019	7.2	Thread start can cause invalid memory writes to arbitrary memory location since the argument is passed by user to kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in MDM9205, MDM9640, MSM8996AU, QCA6574, QCS605, Qualcomm 215, SD 425, SD 427, SD 435, SD 439 / SD 429, SD 450, SD 625, SD	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5128

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2246**		
Out-of-bounds Read	06-11-2019	10	Kernel can do a memory read from arbitrary address passed by user during execution of a syscall in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ8074, MDM9205, MDM9650, QCA8081, QCS605, SD 427, SD 435, SD 450, SD 625, SD 636, SD 665, SD 675, SD 712 / SD 710 / SD 670, SD 730, SD 835, SD 845 / SD 850, SD 855, SD 8CX, SDA660, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130 **CVE ID : CVE-2019-2249**	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5129
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-MDM9-271119/5130

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
msm8909					
Double Free	06-11-2019	7.5	Double free issue can happen when sensor power settings is freed by some thread while another thread try to access. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/5131

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909, MSM8909W, QCN7605, QCS405, QCS605, SDM845, SDX24, SXR1130 **CVE ID : CVE-2019-10565**		
Integer Overflow or Wraparound	06-11-2019	7.5	While processing vendor command which contains corrupted channel count, an integer overflow occurs and finally will lead to heap overflow. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8976, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA845, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM8150 **CVE ID : CVE-2019-2302**	https://source.android.com/security/bulletin/	H-QUA-MSM8-271119/5132
mdm9655					
Improper Validation of	06-11-2019	10	Improper validation of array index causes OOB write and	https://source.android.	H-QUA-MDM9-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, 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-2019-2258**	com/security/bulletin/	271119/5133
sd_410					
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/5134

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
sd_412					
Improper Input Validation	06-11-2019	2.1	While deserializing any key blob during key operations, buffer overflow could occur exposing partial key information if any key operations are invoked(Depends on CVE-2018-13907) in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins	H-QUA-SD_4-271119/5135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909W, 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 625, SD 632, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, 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-2019-2275**		
mdm9635m					
Improper Validation of Array Index	06-11-2019	10	Improper validation of array index causes OOB write and then leads to memory corruption in MMCP in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in MDM9150, MDM9607, MDM9615,	https://source.android.com/security/bulletin/	H-QUA-MDM9-271119/5136

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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-2019-2258**		
Samsung					
galaxy_s8_plus					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung	N/A	H-SAM-GALA-271119/5137

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth, resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**		
Information Exposure	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**	N/A	H-SAM-GALA-271119/5138
galaxy_s3					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth, resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**	N/A	H-SAM-GALA-271119/5139
Information Exposure	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2	N/A	H-SAM-GALA-271119/5140

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**		
galaxy_note_2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow attackers to send AT commands over Bluetooth,	N/A	H-SAM-GALA-271119/5141

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in several Denial of Service (DoS) attacks. **CVE ID : CVE-2019-16400**		
Information Exposure	06-11-2019	3.3	Samsung Galaxy S8 plus (Android version: 8.0.0, Build Number: R16NW.G955USQU5CRG3, Baseband Vendor: Qualcomm Snapdragon 835, Baseband: G955USQU5CRG3), Samsung Galaxy S3 (Android version: 4.3, Build Number: JSS15J.I9300XXUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: I9300XXUGNA8), and Samsung Galaxy Note 2 (Android version: 4.3, Build Number: JSS15J.I9300XUGND5, Baseband Vendor: Samsung Exynos 4412, Baseband: N7100DDUFND1) devices allow injection of AT+CIMI and AT+CGSN over Bluetooth, leaking sensitive information such as IMSI, IMEI, call status, call setup stage, internet service status, signal strength, current roaming status, battery level, and call held status. **CVE ID : CVE-2019-16401**	N/A	H-SAM-GALA-271119/5142
shiftcrypto					
bitbox02					
Information Exposure	02-11-2019	1.9	On SHIFT BitBox02 devices, a side channel for the row-based OLED display was	N/A	H-SHI-BITB-271119/5143

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. Note: BIP39 secrets are not displayed by default on this device. The side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data. **CVE ID : CVE-2019-18673**		
Technicolor					
tc7300.b0					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	3.5	An XSS vulnerability on Technicolor TC7300 STFA.51.20 devices allows remote attackers to inject arbitrary web script via the FileName parameter to /FTPDiag.asp. **CVE ID : CVE-2019-17523**	N/A	H-TEC-TC73-271119/5144

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-11-2019	3.5	An XSS vulnerability on Technicolor TC7300 STFA.51.20 devices allows remote attackers to inject arbitrary web script via the "Connected Clients" field to /wlanAccess.asp. An intranet host can use a crafted hostname to exploit this. **CVE ID : CVE-2019-17524**	N/A	H-TEC-TC73-271119/5145
western_digital					
my_cloud_ex2_ultra					
Out-of-bounds Write	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.183 allows web users (including guest accounts) to remotely execute arbitrary code via a download_mgr.cgi stack-based buffer overflow. **CVE ID : CVE-2019-18929**	N/A	H-WES-MY_C-271119/5146
Out-of-bounds Write	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.183 allows web users (including guest account) to remotely execute arbitrary code via a stack-based buffer overflow. There is no size verification logic in one of functions in libscheddl.so, and download_mgr.cgi makes it possible to enter large-sized f_idx inputs. **CVE ID : CVE-2019-18930**	N/A	H-WES-MY_C-271119/5147
Buffer Copy without Checking Size of Input ('Classic Buffer	13-11-2019	9	Western Digital My Cloud EX2 Ultra firmware 2.31.195 allows a Buffer Overflow with Extended Instruction Pointer (EIP) control via crafted GET/POST	N/A	H-WES-MY_C-271119/5148

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			parameters. **CVE ID : CVE-2019-18931**		
ZTE					
mf910s					
Information Exposure	07-11-2019	1.9	The Sec Consult Security Lab reported an information disclosure vulnerability in MF910S product to ZTE PSIRT in October 2019. Through the analysis of related product team, the information disclosure vulnerability is confirmed. The MF910S product's one-click upgrade tool can obtain the Telnet remote login password in the reverse way. If Telnet is opened, the attacker can remotely log in to the device through the cracked password, resulting in information leakage. The MF910S was end of service on October 23, 2019, ZTE recommends users to choose new products for the purpose of better security. **CVE ID : CVE-2019-3422**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011722	H-ZTE-MF91-271119/5149
zxupn-9000e					
Incorrect Default Permissions	08-11-2019	7.5	The 9000EV5.0R1B12 version, and all earlier versions of ZTE product ZXUPN-9000E are impacted by vulnerability of permission and access control. An attacker could exploit this vulnerability to directly reset or change passwords of other accounts.	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011683	H-ZTE-ZXUP-271119/5150

CV Scoring Scale (CVSS)	0-1	1-2	2-3	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-2019-3425		
Improper Input Validation	08-11-2019	7.5	The 9000EV5.0R1B12 version, and all earlier versions of ZTE product ZXUPN-9000E are impacted by the input validation vulnerability. An attacker could exploit this vulnerability for unauthorized operations. **CVE ID : CVE-2019-3426**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1011683	H-ZTE-ZXUP-271119/5151
Zyxel					
p-1302-t10d					
Incorrect Authorization	12-11-2019	4	ZyXEL P-1302-T10D v3 devices with firmware version 2.00(ABBX.3) and earlier do not properly enforce access control and could allow an unauthorized user to access certain pages that require admin privileges. **CVE ID : CVE-2019-15815**	https://www.zyxel.com/support/P1302-T10D-v3-modem-insecure-direct-object-reference-vulnerability.shtml	H-ZYX-P-13-271119/5152

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10